روسيا والولايات المتحدة

الدبلوماسية الالكترونية الطريق لفتح الابواب

الطبعة الأولى

1436هـ - 2015م



الأكاديميون للنشر والتوزيع

المملكة الأردنية الهاشمية

عمان – مقابل البوابة الرئيسية للجامعة الأردنية

تلفاكس : 0096265330508

جـوال : 00962795699711

E-mail: academpub@yahoo.com

This Stady Was Published in English Language by The institute of East and West Studies

الدراسة صدرت باللغة الانجليزية من قبل

معهد دراسات الشرق والغرب

(EWI - NEW YORK)

رقم الإيداع لدى المكتبة الوطنية

2014 / 7 / 3259

رقم التصنيف:327.37047

المؤلف ومن في حكمه:

معهد دراسات الشرق والغرب

ترجمة: طارق محمد الطائي

الناشر

الأكاديميون للنشر والتوزيع

عمان – الأردن

عنوان الكتاب:

روسيا والولايات المتحدة الدبلوماسية الالكترونية

الطريق لفتح الأبواب

الواصفات:

العلاقات الدولية// الولايات المتحدة// روسيا/

ISBN : 978-9957-590-04-8

بسم الـلـه الرحمن الرحيم

(يَرْفَـعِ الـلــهُ الَّـذِينَ آمَنُـوا مِـنكُمْ وَالَّـذِينَ أُوتُـوا الْعِلْـمَ دَرَجَـاتٍ وَالـلـهُ بِمَا تَعْمَلُونَ خَبِيرٌ {11/58})

صدق الـلـه العظيم

سورة المجادلة :(11)

روسيا والولايات المتحدة

الدبلوماسية الإلكترونية

الطريق لفتح الأبواب

تأليــف

فرانز ستيفن وغريغ أوستين

ترجمـــة

طــارق محمـد ذنـون الطائـي

كلية العلوم السياسية - قسم العلاقات الدولية

جامعة الموصل



الأكاديميون للنشر والتوزيع

تقديم

يقدم التقدم التكنومعلوماتي وطرق اختراق منظومات الدول الأخرى المادية والمعنوية ، العسكرية والأمنية الالكترونية شكلا للدبلوماسية يواكب متطلبات العصر ، مما يجعل الدبلوماسية التقليدية بآليتها وتقاليدها المتمثل بعالم الرقي والثقافة واللياقة والجمال جزءا من الإرث التاريخي البشري الجميل . الموضوع يقدم جهدا رائعا ، وتكمن أهميته في اكتشاف ما يحتويه من طروحات وأفكار تتناغم ولغة العصر وأزماته وصراع المصالح الحيوية بين القوى الدولية والرؤيا الإستراتيجية لها لاسيما فيما يتعلق بإيجاد دبلوماسية معاصرة تتمثل بدبلوماسية الأمن الالكتروني.

د. محمود سالم السامرائي

أستاذ الدراسات الدولية المساعد

جامعة الموصل / كلية العلوم السياسية / قسم العلاقات الدولية

في خضم الانجازات العلمية والتكنولوجية الهائلة التي تحققت منذ بداية الربع الأول من القرن الواحد والعشرين ، ظهرت الانعكاسات واضحة جلية على العديد من مجالات الحياة ، ومن ذلك علاقات التفاعل الدولي في جوانبها السياسية والإستراتيجية والاقتصادية ، من خلال تبني العديد من الآليات والتدابير المتعلقة بالأمن الالكتروني ومواجهة التهديدات المنصبة على امن المعلومات . وفي ضوء ذلك ظهرت الدبلوماسية الالكترونية بوصفها نمطا جديدا

أو غير مسبوق لنشاط دولي بدأ يشكل السمة الأساسية لعصرنا الحالي . والمتغير الأكثر تأثيراً في التفاعلات الدولية وفي علاقات الصراع والقوة بين الفواعل الدولية المختلفة.

د. صلاح حسن محمد

أستاذ العلاقات الدولية المساعد

جامعة الموصل / كلية العلوم السياسية / قسم العلاقات الدولية

اطلعت على كتاب روسيا والولايات المتحدة (الدبلوماسية الالكترونية الطريق لفتح الأبواب) لفرانز ستيفن وغريغ اوستين... والحق أقول أن الأستاذ طارق محمد ذنون الطائي مترجم الكتاب قد أجاد ايما إجادة في اختيار هذا الكتاب ليسهم إسهاما لا يقل عن جهد المؤلفين في اغناء المكتبتين العراقية والعربية اغناءاً معمقاً في موضوع بات يمثل المفصل الحقيق للأداء السياسي والاستراتيجي الفاعل للقوى الكبرى والعظمى المتنافسة والمتصارعة في عالم اليوم...

العالم الذي لم يعد يتقبل سوى القوى الكفؤة طبقا لمعايير العلم والمعرفة المتقدمة الراقية ، إذ بات الأمن العالمي في عصرنا متجاوزا للمرتكزات التقليدية وصولا إلى مخرجات ثورة المعلومات مما يتيح لنا القول أن الأمن العالمي بات أمنا معلوماتياً الكترونياً والصراع هو الآخر اتخذ المنحنى نفسه ، وكذا الحال للحروب ومظاهر التفاعلات الدولية الأخرى .

إن ترجمة هذا الكتاب بالمستوى اللائق والرفيع لغة وأسلوبا يعد بحد ذاته انجازاً أتاح التواصل مع المستجدات العلمية والمعرفية ، ولعل الشكر هو اقل ما يسدى إلى الأستاذ طارق محمد ذنون الطائي مترجم الكتاب...

د. سرمد زكي الجادر

أستاذ الإستراتيجية والشؤون الدولية

جامعة النهرين / كلية العلوم السياسية

في ظل عصر المعلومات أصبحت العلاقات الدولية تتسم بسيادة المعرفة والتقدم التكنولوجي ، وهو ما جعله معياراً هاما للأداء الدبلوماسي للدولة . إذ لم تعد الدول قادرة على السيادة والتحكم في عملية تدفق المعلومات إلى داخلها ، وبين سلبيات وايجابيات هذه المرحلة وفرضياتها وقيودها أصبح من الطبيعي أن تلجأ الدول التي تمتلك هذه المعرفة لاستخدامها في الأداء الدبلوماسي . وعلى عكس مدة الحرب الباردة التي وضعت فرضيات وقيود في تعامل الولايات المتحدة والاتحاد السوفيتي ، فإن عالم القرن الواحد والعشرين قد وضع فرضيات جديدة في التعامل الأمريكي الروسي في المجال الدبلوماسي . وتحاول هذه الدراسة المترجمة تزويد القارئ العربي بخفايا هذه الدبلوماسية واستخداماتها . ومن ثم تطرح هذه الدراسة القيمة أمامنا سؤالا في غاية الأهمية : أين نحن مما يجري في العالم ؟

د. طارق محمد طيب

رئيس قسم العلاقات الدولية

جامعة الموصل / كلية العلوم السياسية / قسم العلاقات الدولية

المقدمة

آياً كان تعريف الدبلوماسية أو أصلها، سواء في كونها علم وفن المفاوضات أم آلية السياسة الخارجية للدول، فان مضمونها يتحقق من خلال أدرك وظيفتها، بل أهميتها ودورها في العلاقات بين الدول والمنظمات الدولية والإقليمية، وكذلك الهدف لتحقيق المصالح بالطرق والوسائل السلمية.

والبعض يرى أنها "مجموعة المفاهيم القواعد والإجراءات والمراسم والمؤسسات والأعراف الدولية التي تنظم العلاقات بين الدول والمنظمات الدولية والممثلين الدبلوماسيين بهدف خدمة المصالح العليا للدول".

وفي كون الدبلوماسية أداة للسياسة الخارجية للدول فقد تنوعت أنماطها وتعددت أشكالها فهي لم تعد ذلك النمط التقليدي المتمثل بنشاط البعثة الدبلوماسية ممثلة بسعادة السفير، وإذا ما تجاوزنا الأنماط التقليدية للدبلوماسية وبخاصة في عالمنا المعاصر، لنجد أشكالاً وأنماطاً مختلفة منها:

"دبلوماسية القمة"(Summit Diplomacy) أو المؤتمرات التي يعقدها رؤساء الدول لمناقشة بعض المسائل أو القضايا الدولية أو العلاقات بين الدول المشتركة في لقاء القمة. وهذا في الواقع الدولي المعاصر يعكس مدى التطور في أهمية العلاقات بين الدول ومنظماته بشكل عام، ودبلوماسية لقاءات القمة تشكل اليوم احد أهم الوسائل بقصد وضع حلول أو عقد اتفاقيات بين الدول، حيث أن لقاء قادة الدول وبما لديهم من صلاحيات واسعة ما يساعد على اختزال الزمن بالتوصل إلى قرارات هامة.

والشكل الآخر هو "دبلوماسية الأزمات"(Crisis Diplomacy) ويقصد بها الدبلوماسية التي تسعى لحل أزمة دولية أو إقليمية طارئة. وإدارة الأزمات الدولية أصبحت ذات أهمية كبيرة في العلاقات الدبلوماسية المعاصرة. ذلك لان المجتمع الدولي المعاصر بات يواجه باستمرار أزمات سياسية مختلفة نتيجة للاختلاف في المصالح.

وشكل أخر هو "دبلوماسية التحالفات"(Alliance Diplomacy) وهي تعني النشاط الدبلوماسي الهادف بقصد أنشاء تحالفات سياسية وتكتلات سياسية، وعسكرية، لان المجتمع الدولي المعاصر يعيش في ظل اضطراب امني وصراع للقوى لذا تصبح دبلوماسية التحالفات من الأهمية لأمن الدول ومصالحها الحيوية ونفوذها لذا حظيت باهتمام خاص في مجال التحالفات.

وشكل جديد بات أكثر حيوية "الدبلوماسية الرقمية "(Cyber Diplomacy) التي لا تختلف كثيراً عن الدبلوماسية التقليدية المتعارف عليها من حيث أهدافها، بل ما يميزها هو المشاركة الفاعلة للشعوب في تقديم المشاكل ومتطلبات العصر للشعوب وواقعها بفضل شبكات التواصل الاجتماعي ومخاطرها وتداعياتها على أسرار الدول لاسيما الكبرى منها؛ وفي ذات الوقت أصبح مهماً بالنسبة للمؤسسات الحكومية أكثر مما مضى أن يكون لها تواجد فعال على هذه الشبكات، لا لقمع هذه الأصوات، وإنما للاستماع إليها ولهمومها وتقييم ردود الأفعال وبناء فكرة أفضل عن آمال الشعوب لتتوافق مع مصالح المجتمعات للصالح العام.

فالتقـدم التكنومعلومـاتي وطـرق اخـتراق منظومـات الـدول الأخـرى الماديـة والمعنويـة العسكرية والأمنية الالكترونية يقدم للدبلوماسـية شـكلا يواكـب متطلبـات العـصر، مـما يجعـل الدبلوماسية التقليدية بآليتها وتقاليدها المتمثل بعالم الرقي والثقافة واللياقة والجـمال جـزأ مـن الإرث التاريخي البشري الجميل.

الموضوع يقدم جهدا رائعا، وتكمن أهميته في اكتشاف ما يحتويه مـن طروحـات وأفكـار تتناغم ولغة العصر وأزماته وصراع المصالح الحيوية بين القوى الدوليـة والرؤيـا الإسـتراتيجية لهـا لاسيما فيما يتعلق بإيجاد دبلوماسية معاصرة تتمثل بدبلوماسية الأمن الالكتروني.

د. محمود سالم السامرائي

أستاذ الدراسات الدولية المساعد

جامعة الموصل/ كلية العلوم السياسية

قسم العلاقات الدولية

توطئة

يعد الأمن الدولي الالكتروني من الموضوعات المهمة في الدراسات الإستراتيجية، إذ انه يتميز بالطابع العلمي، كما انه يتميز بكونه امناً شاملاً يمس المجتمع الدولي وشعوب ومؤسسات وقطاع خاص. كما أن التحولات والمؤثرات الإستراتيجية الدولية مترابطة وتتميز بسمة الانتقال السريع وفي مدة زمنية محددة بفعل المتغيرات الهائلة التي وفرتها البيئة الدولية في القرن الحادي والعشرين بمتغيراتها الاقتصادية والعسكرية والمعلوماتية والتكنولوجية والحضارية وغيرها.

هذه المتغيرات مترابطة بطبيعتها وتتفاعل مع بعضها، فتارة تقوي بعضها وتارة أخرى تقوض بعضها الأخر.

يعد الأمن الالكتروني كما يفضل السياسيون الأمريكيون تسميته أو الأمن المعلوماتي كما يفضل الروس تسميته من المتغيرات المؤثرة في التفاعلات الإستراتيجية الدولية بوصفه عاملاً يتسم بالتطور والتجدد، كما انه يرتبط بالتقدم التكنولوجي بوصفه احد المتغيرات المستقبلية التي سوف تتحكم بمكانة القوى الدولية في هذا القرن. فضلا عن أن معظم اتفاقيات الدفاع المشترك لم تتضمن نصوصها على الدفاع المتبادل إذا ما تعرضت الدول المنظمة إلى الاتفاقية إلى هجوم الكتروني.

إن الأمن الالكتروني يترك وسوف يترك أثره بشكل فاعل على مجمل التفاعلات الدولية، إذ انه سوف يؤثر على الدائرة الأولى (الدولة ذات السيادة) والدائرة الثانية (النظم الإقليمية في العالم) والدائرة الثالثة (الدائرة العالمية) نتيجة ترابط هذه الدوائر الثلاثة بفعل إزالة الحواجز التي كانت قائمة في القرن

العشرين، كما أن ذلك سيكون له تداعيات سلبية وايجابية على الأمن الالكتروني الدولي، فعلى الرغم من أن التقدم في مجال المعلومات والتكنولوجيا وارتباطها بشبكة المعلومات الدولية أسهم في خلق فرص جديدة توظف في الحفاظ على أنظمة الدوائر الثلاثة التي سبق ذكرها فإنها في الوقت نفسه أوجدت تحديات جديدة لهذا الأمن.

لقد اوجد الأمن الالكتروني فرص وتحديات جديدة في حياة الإنسان والمجتمع والدولة والمجتمع الدولي وهرمية القوى الدولية، إذ إنها عملت على إلغاء المسافات بين الوحدات الدولية بفعل ارتباطها بالتقدم العالمي والتكنولوجي، فضلاً عن أن الدول عملت على استخدام هذا العامل بالشكل الذي يحقق مصالحها في البيئة الدولية بأساليب مختلفة شرعية وغير شرعية وهنا تتضح درجة ارتباطها بالأمن الدولي ونتائجه المستقبلية على التفاعلات الدولية. ذلك إن المصلحة الذاتية للدول تدفعها إلى توظيف التقنيات الالكترونية المتطورة بهدف الحفاظ على أمنها وتعزيز قوتها الذاتية، لا بل تعمل على اختراق منظومة الأمن القومي للدول والوحدات الفاعلة الأخرى في العلاقات الدولية من اجل تحقيق مصالحها الإستراتيجية العليا والسيطرة على سلوكيات الدول الأخرى، وهو الأمر الذي يزيد من تعرض الدول والمؤسسات الدولية بصنوفها الاقتصادية والمالية والإدارية إلى تحديات غير مدركة لتحدياته وتهديداتها المستقبلية، ومن ثم فان هذا الفعل ورد الفعل الالكترونية الناجمة عن الاستهداف المتبادل تسهم في زيادة تحديات الأمن الدولي.

وإذا تحكم العامل العسكري في معطيات التفاعلات الدولية خلال مدة الحرب الباردة، ومن ثم العامل الاقتصادي بعد ذلك، أي في العقد الأخير من القرن العشرين، فان المستقبل هو للدول التي تمتلك القدرات التكنولوجية

المتقدمة، وتتمكن من توظيفها في المجالين السابقين (الجانب العسكري والجانب الاقتصادي). ذلك أن التجسس الصناعي والمعلوماتي تحول في مرحلة ما بعد الحرب الباردة من كشف الأسرار السياسية والعسكرية إلى مرحلة جمع المعلومات عن المنافسين لا سيما فيما يتعلق بالصراعات الاقتصادية، فضلاً عن الاعتماد على تقنية المعلومات في حروبها المختلفة، وهو الأمر الذي سيزيد من حالة عدم الاستقرار في العلاقات الدولية، أي سوف يجعل من السلام والتعاون ليس الحالة الدائمة في العلاقات الدولية.

تتمثل الجوانب السلبية للأمن الالكتروني في مصادرة سيادة الدولة، وسعي الدولة إلى التوظيف السلبي التجسسي لشبكة المعلومات الدولية، فضلاً عن مصادرة الخصوصيات والقرصنة الالكترونية، وأخيرا وليس أخرا العمل على توظيفها في الحروب المستقبلية.

أي بمعنى أن التكنومعلوماتية المرتبطة بالالكترونية أصبحت احدي المتغيرات الحاكمة للاستراتيجيات الدولية، ومن ابرز هذه الاستراتيجيات هي الإستراتيجية الأمريكية والإستراتيجية الروسية، وتحاول الدولتان التحكم بمتغيرات النظام الدولي في القرن الحادي والعشرين، فالدولتان هما الأقوى في العالم بفعل امتلاكهما لمقدرات القوة الشاملة (السياسية والاقتصادية والعسكرية والمعرفية) ومن ثم فأنهما يملكان التأثير الفاعل في التفاعلات الدولية في القرن الحادي والعشرين.

إن أهمية الدراسة التي شرعنا بترجمتها تكمن في أنها تناولت احد الموضوعات غير تقليدية في الدراسات الإستراتيجية، ذلك أن علم الإستراتيجية اخذ مديات وأبعاد لم تكن منظورة قبل مدة من الزمن، ومن أبرزها الأمن

الالكتروني. كما أنها في طابعها العام تركز على العلاقات التفاعلية بين الولايات المتحدة وروسيا الاتحادية وتحديدا الدبلوماسية الالكترونية.

وعلى الرغم من بعض الصعوبات التي واجهت الباحث أثناء عملية الترجمة إلا انه حاول قدر الإمكان الاقتراب من المعنى بهدف إيصال المغزى إلى القارئ العربي بسهولة ويسر.

ويسعني أن أتقدم بالثناء والاحترام إلى الدكتور محمود سالم السامرائي أستاذ الدراسات الدولية الذي تولى التقديم لهذا الجهد، فضلاً عن ملاحظاته المتعلقة بترجمة النصوص المتعلقة بالعلوم السياسية والدراسات الإستراتيجية، والدعم والرأي الذي أبداه كل من الدكتور صلاح حسن محمد والدكتور سرمد زكي الجادر والدكتور طارق محمد طيب رئيس قسم العلاقات الدولية في كلية العلوم السياسية/جامعة الموصل فيما يتعلق بمضمون ومحتوى الكتاب. والثناء موصول إلى المقوم اللغوي الأستاذ حسام لجهوده الطيبة في إخراج هذا الجهد سليماً من الناحية التعبيرية واللغوية.

طارق محمد ذنون الطائي

مدرس العلاقات الدولية المساعد

جامعة الموصل/ كلية العلوم السياسية

قسم العلاقات الدولية

شكر وثناء....

تستند النتائج التي توصلت إليها الدراسة إلى المشاورات التي جرت على مدار السنة في موسكو وواشنطن وبروكسل. وقد أجرى فرانز ستيفن عدة مقابلات في موسكو في آذار من عام 2010 مع كبار المتخصصين الروس في مجال الأمن الالكتروني من القطاعين العام والخاص. إن المؤلفين يودا أن يشكرا الدكتور فاليري بستشينكو النائب الأول لرئيس جامعة موسكو الحكومية ومعهد الأمن المعلوماتي، وديمتري غربيعوف المستشار السياسي لمدير معهد الأمن ألمعلوماتي، وفلاديمير دينزيخكن وليوند زحوكوف المدير التنفيذي وباشا شاركوف زميل معهد الدراسات الأمريكية الكندية وفلاديمير سوكولوف نائب مدير الأمن ألمعلوماتي. كما يود المؤلفان أن يتوجها بالشكر إلى ليزا كور كولسيوري وفلاديمير ايفانوف وغالينا كوليكوفا وبنيامين بارير وبابولو روديغوز وسيم جين ويميلس من معهد دراسات الشرق والغرب لمشاركتها في أجراء المقابلات. فضلاً عن تعليقاتهم ودعمهم في مجال البحث.

خلاصة تنفيذية:

لم تـتمكن روسـيا الاتحاديـة والولايـات المتحـدة مـن تأسـيس فهـم مـشترك في مجـال دبلوماسيتها الثنائية حول معظم جوانب الأمن الالكتروني. فعـلى الـرغم مـن إعـلان 1998 الـذي يؤكد على الرغبة المـشتركة لقيـادة عمليـة الاسـتجابة العلميـة لتحـديات الأمـن الالكـتروني، فـان البلدين عملا وتصرفا على أنهما أعداء يحرسون الأسرار الوطنية الأمنية الحساسة بدلاً من كـونهما حلفاء يلتزمون بحماية المصالح المشتركة في الاقتصاد العالمي الرقمي والـشبكة العالميـة المترابطـة اجتماعياً.

يمكن القول أن هنـاك سـوابق تاريخيـة دامغـة تؤكـد بـان التحفظـات لـدى كـل روسـيا الاتحادية والولايات المتحدة والتي تعد متجـذرة وتتمثـل في حـساسيات الأمـن الـوطني، ويمكـن التغلب عليها وتخطيها. فعلى سبيل المثال، في مجال الأعداد لـ Y2k، فان هناك تهديدا عالميا كبير، وان معظم الدول تعاونت على الرغم من حساسيات الأمن الوطني.

لقد تبنت الولايات المتحـدة وروسـيا الاتحاديـة تـدابير متداخلـة لتحقيـق المراقبة المشتركة حول معظم إجراءات الانطلاق والتحذير فيما يتعلق بالـصواريخ الباليستية. وفي الآونة الأخيرة، اتفقت الولايـات المتحـدة وروسـيا الاتحاديـة عـلى ترتيـب تغـيرات مـشتركة جديـدة لمـدة أربعـين عامـاً حـول الخـط الـساخن بـين الكرملين والبيت الأبـيض. فـضلا عـن ذلـك، تعاونـت مـصارف الولايـات المتحـدة

وروسيا الاتحادية علـى تـأمين الاتـصالات الرقميـة لعمليـات النقـل الـدولي للمبـالغ الكبـيرة مـن الأموال.

إن الولايات المتحدة وروسيا الاتحادية تعالجان مخرجـات الأمـن الالكـتروني مـن زاويتـين مختلفتين: إذ تركز الولايات المتحدة على منهج تنفيذ القانون على المـستوى المحـلي مـع التعـاون الدولي الطوعي، بينما تركز روسيا الاتحادية على تطوير الأنظمة الدوليـة الملزمـة. كـما أن هنـاك فلـسفات مختلفـة في العمـل، إذ تفـضل روسـيا الاتحاديـة الـسيطرة الاجتماعيـة عـلى الانترنـت كوسيلة، بينما ترفض الولايات المتحدة هذه الوسيلة.

وعلى الرغم من هذه الاختلافـات فقـد اتفقـت الولايـات المتحـدة وروسـيا الاتحاديـة في كانون الأول من عام 2009 في اجتماع لجنـة الأمـم المتحـدة حـول نـزع الـسلاح النـووي والأمـن الدولي على البدء في محادثات حـول تعزيـز امـن الانترنـت والحـد مـن الاسـتخدام العـسكري في المجال الالكتروني.

ونتيجة رفض روسيا الاتحادية الاقتراحات المتعلقة بـالأمن الالكـتروني لـسنوات عـدة فـان الولايات المتحدة قررت بشكل واضح تغير سياستها بـشكل كبـير، إذ أعلنـت عـن أهـداف الأمـن الالكتروني في أيار من العام 2009، وقد أظهرت إدارة اوباما عزمها على تركيز اهتمامها على الأمن الالكتروني والوصول إلى مستوى جيد. وعلى هذا الأساس، فانه يمكن التوصل إلى اتفاقات جديـدة بين الولايات المتحدة وروسيا الاتحادية.

أن الهدف النهائي لهذه الدراسة هو أن هذه المناقشات هي من اجل الدفع باتجاه تقـدم سريع وواسع لاسيما في مجال الأمن الالكتروني، أو كما يفضل الروس تـسميته بـالأمن المعلومـاتي. كما أنها تحث الطرفين على تبني إعلانهما العام في كانون الأول من عام 2009 التي من شـأنها أن تدفع باتجاه البدء بمشاورات جديدة تتعلق بالأمن الالكتروني بالاستناد الى قرار الجمعيـة العامـة للأمم المتحدة.

وبهدف تشخيص العوائـق وطـرق التغلـب عليهـا فـان الدراسـة تنـاقش أربعـة مجـالات ممكنـة للتعـاون مـن أهمهـا : البنيـة التحتيـة الأساسـية العامـة، والاسـتجابة الـسريعة للجريمـة الالكترونية، والمداولات التي تقوم بها منظمة الأمن والتعاون الأوربية حـول الحـرب الالكترونيـة، وأخيرا التعاون بين روسيا الاتحادية وحلف شمال الأطلسي في مجال الأمن الالكتروني.

التوصيات

تتمثل التوصيات التي تم إدراجها في أدناه في الاقتباسات الواردة في البيان المعلن من قبل الجانبين وسعيها للعمل جنباً إلى جنب من اجل تطبيقه بهدف قيادة التغيير في كل مجال من المجالات الأربعة.

تحث هذه الدراسة الحكومتين على أن تقوم كل منهما باقتراح مبادرة في محفل دولي مناسب (على سبيل المثال الاتحاد الدولي للاتصالات السلكية واللاسلكية)، وترؤس مجموعات العمل اللازمة وإشراك جميع الأطراف ذات العلاقة في المناقشات بهدف بناء الثقة وتعميق التعاون. وينبغي أن يعقب ذلك مناقشات ثنائية ملموسة حول جوانب محددة للتعاون وتعد جوانب حساسة في أي منتدى دولي:

1- البنية التحتية الأساسية العامة: يجب أن تشجع الولايات المتحدة الأمريكية وروسيا الاتحادية في إطار الاتحاد الدولي للاتصالات السلكية واللاسلكية فكرة عقد اتفاقية ملزمة متعددة الأطراف حول البنية الأساسية العامة بهدف تعزيز النظام الاقتصادي للهويات الموثقة دولياً. وهذا بدوره يجب أن يرتكز على التقييم السياسي المشترك لخبراء روسيا الاتحادية والولايات المتحدة الأمريكية.

2- الاستجابة السريعة للجريمة الالكترونية: يجب أن تعمل الولايات المتحدة وروسيا الاتحادية على توسيع البنى التحتية لشبكة الاتصالات المتعلقة

بجرائم التكنولوجيا المتقدمة على مدار الساعة، وتحت مظلة مجموعة الثماني بالتوافق مع تشجيع الإطار العالمي للاتصال 7/24 وبضمنها دعم البرنامج العالمي لبناء القدرات في مجال تنفيذ القانون والتحقيق في مجال الجرائم الالكترونية لكل الدول المرتبطة بشبكة المعلومات الدولية.

3- القانون الدولي الالكتروني: يجب على الولايات المتحدة وروسيا الاتحادية أن تشرفا على سياسة تقييم الجوانب القانونية المرتبطة بتنظيم نشاطات الحرب الالكترونية الدفاعية والهجومية لاسيما فيما يتعلق بالبنى التحتية المهمة " قواعد الاشتباك"، إن اختيار المنتدى المناسب لذلك هو بحد ذاته معضلة كبيرة، ولكن مع ذلك، فان أفضل الخيارات من سلسلة الخيارات الضعيفة يمكن أن تكون منظمة الأمن والتعاون الأوربية.

4- التبادلات والمناورات العسكرية الالكترونية بين روسيا الاتحادية وحلف شمال الأطلسي: على المستوى السياسي يجب أن تلتزم الولايات المتحدة وروسيا الاتحادية بانجاز التقييم المشترك في الإطار الزمني المحدد (سنتان) حول ما الذي يشكل الأمن الالكتروني وكيف يمكن تحقيقه. وفي إطار التعاون العلمي بين روسيا الاتحادية وحلف شمال الأطلسي، فانه يجب أن تشترك الولايات المتحدة وروسيا الاتحادية في المراقبة المتبادلة والمشاركة في محاكاة الهجمات الالكترونية. كما يجب على الدولتين وبالاشتراك مع حلف شمال الأطلسي أن تطوروا منهجيات ومعاييراً لتقييم مدة التأثير وترتيب المرافق الحيوية الحساسة.

المحور الأول:من حرب التجسس والحرب الالكترونية إلى الدبلوماسية الالكترونية

نحن نواجه مخاطر معاصرة واضحة المعالم في العالم الرقمي: إذ تؤكد المعلومات من المصادر السرية على زيادة حجم ونطاق التهديدات بشكل يثير القلق أكثر من المشاكل السابقة. وهذه ليس حالة مثيرة للذعر. وعلى أية حالة العكس صحيح. إذ إن تأخر الإدراك العام لهذا الخطر كان وراء هذه الحقيقة.

لقد أوضح الرئيس الأمريكي باراك اوباما أثناء إعلان سياسة الأمن الالكتروني الجديدة في 2009/5/29 مدى شعور الولايات المتحدة بتصاعد قدرتها الدفاعية. فقد قال (نحن لم نستعد كما يجب) ولذلك (نحن فشلنا في الاستمرار في مجال الأمن في بنيتنا التحتية الرقمية. وفي تقرير صدر في كانون الأول من عام 2009 من قبل لجنة تم تشكيلها من قبل مركز الدراسات الإستراتيجية والدولية (CSIS) في واشنطن تحت عنوان (الحرب الالكترونية: المعركة الخفية) وهي مشابهة للإشارات المعلوماتية في الحرب العالمية الثانية. وقد توصلت اللجنة بان (الفشل الأمريكي في حماية الفضاء الالكتروني يعد احد مشاكل الأمن القومي).

وفي عام 2000 وقع الرئيس الروسي فلاديمير بوتين (عقيدة الأمن المعلوماتي) التي توصلت من جملة ما توصلت إليه إلى ما يأتي:

1- هناك تدهور لحالة امن البيانات التي تشكل أسرار الدولة.

2- إن معظم العلماء المتخصصين والمؤهلين تركوا هذا المجال في روسيا الاتحادية.

3- إن التخلف في مجال تكنولوجيات المعلومات الوطنية يدفع الحكومة على شراء المعدات الأجنبية ومن ثم يزيد من احتمال الحصول عليها بطرق غير شرعية.

4- تزايد الاعتماد الروسي على الحواسيب الأجنبية والاتصالات السلكية واللاسلكية والصناعات المرئية والصلبة.

5- تزايد التهديدات باستخدام (السلاح المعلوماتي ضد روسيا الاتحادية).

6- انعدام التنسيق الكافي، والميزانية المتواضعة لا تلبي الحاجة للمواجهة الوطنية لهذه التهديدات.

7- ليس هناك اهتمام كاف فيما يتعلق بتطوير نظم استطلاع وانظمه الحرب الالكترونية.

إن عوامل الوهن كبيرة جداً وتشمل جميع الأطراف، بدءاً من المعلومات الشخصية والسجلات المصرفية والسيطرة على الأدوات الطبية الحساسة مروراً بمحطات الطاقة النووية والصواريخ الباليستية النووية. وفي كل هذه المجالات، يمكن أن تجد قصص الرعب التي تحدث على مدى العقد الأخير من الزمن. وقد

أشارت التقارير أن احد القراصنة تمكن من سحب التصاميم السرية لواحدة من أحدث الطائرات العسكرية الأمريكية.

وبهدف حماية البيانات وشبكات المعلومات تبنت الولايات المتحدة وروسيا الاتحادية فضلاً عن دول أخرى استراتيجيات متعددة رئيسة وفرعية من اجل تعزيز البنية الدفاعية. وهذا منهج يستحق الاهتمام أكثر من الاهتمام في عهد العصور الوسطى وهو العصر الالكتروني وهو عصر قابل للفهم والإدراك.

لا تزال الولايات المتحدة وروسيا الاتحادية تبذلان جهوداً كبيرة من اجل جمع المعلومات عن بعضهما الآخر، وكل دولة تحاول إخفاء عملية تطوير تقنيات الأسلحة عن الأخرى، كما أن كل منهما يشرف على عمليات الهجوم الالكترونية ضد الأخر. إن الأمن الالكتروني يجب أن ينظر إليه على انه حالة من حالات الدفاع الجيدة. والجدران النارية تعمل بوصفها الدفاعات الحركية المقابلة وسوف تستمر في لعب هذا الدور. نحن في عهد المواجهة العسكرية أو على الأقل عصر الصدامات التي تحدث في مجالات يصعب التحكم بها، إذ ن المجالات التقليدية المتمثلة بالأرض والبحر والجو والغلاف الجوي تحكمها ضوابط لتحقيق الأمن، بينما لا يتوفر ذلك في المجال الالكتروني.

ونتيجة المستويات العالية للاتصالات العابرة للحدود في المجال الالكتروني فانه لابد من وجود منهجيات للأمن القومي الالكتروني قادرة على العمل في المجال الدولي. ونتيجة لذلك، فانه لابد من البدء بتطوير الدبلوماسية الالكترونية.

إن عددا ضئيلا من الحكومات لديها معرفة عن البعد الدبلوماسي للأمن الالكتروني، ومـن ثم بالتأكيد ليس لديها اسـتراتيجيات دبلوماسـية متطـورة بمـا يتناسـب مـع التهديـدات. كـما أن معظم الحكومات لم تقم إلا بالقليل في المجال الدبلوماسي في هذا العـصر الجديـد (عـصر الأمـن الالكتروني).

لقد جاءت الدراسة لتعـالج جـزءاً مـن المـصلحة الأمريكيـة الروسـية المعلنـة وتتمثـل في القيادة المشتركة من اجـل التغلـب عـلى التحـديات العالميـة في مجـال امـن المعلومـات وشـبكة الانترنت. وفي عام 1998 أصدر رئيسا كل من الولايـات المتحـدة وروسـيا الاتحاديـة بيانـاً مـشتركا حول تحديات الأمن المشتركة في بداية القرن الحادي والعشرين. وقد أشاروا فيه إلى أهمية تعزيز الجوانب الايجابية والتخفيف مـن الجوانـب الـسلبية للثـورة التكنومعلوماتيـة التـي تجـري الآن والتي تعد تحدياً خطيرا لضمان مستقبل مصلحة الأمن الاستراتيجي لهما. كما أنهم التزما رسـمياً. من اجل العمل معا فيما يتعلق بمشكلة Y2k، فضلاً عن أنهما وضعا التزاماً عامـاً بهـدف التعبئـة العامة لجهود المجتمع الدولي بأسره واستخدام كل الموارد الضرورية للقيام بذلك. وتعهدا بـأنهما سوف يستمران في لعب دور قيادي وثنائي ومتعدد الأطراف لتحقيق الأهداف المشتركة في مجـال الأمن.

وقد تم وضع بداية جيدة في إطار بذل الجهود من اجل منع الجريمة الالكترونيـة. ولكـن البداية الأولى لمعاهدة دولية في هذا المجال هي اتفاقية المجلس الأوربي حول الجريمة الالكترونية التي فتح التوقيع عليها في2001/10/23.

لقد صممت هذه الاتفاقية لتعالج أصناف عديدة من الجرائم المرتكبة عن طريق شبكة المعلومات الدولية والحاسوب. وقد وقعت الولايات المتحدة وصدقت على المعاهدة ولكن روسيا الاتحادية لم توقع عليها. (تسعة وعشرون بلداً صادقوا على الاتفاقية التي دخلت حيز التنفيذ في عام 2004). كما أن المملكة المتحدة لم توقع على المعاهدة حتى الآن. إن روسيا الاتحادية تتعاون بشكل فعلي مع التحقيق في الجرائم الدولية وحققت نتائج ايجابية، ولكنها لم تكرس الموارد الكافية كما تفعل الولايات المتحدة ذلك.

في عام2006، وخلال رئاستها لمجموعة الثمانية، قدمت روسيا الاتحادية مبادرة من اجل تحقيق شراكة بين القطاع العام والخاص بهدف مواجهة الإرهاب والجريمة المنظمة والأمن الالكتروني التي كانت واحدة من الأولويات الثلاثة جنباً إلى جنب مع حماية البنية التحتية للطاقة الحساسة، فضلا عن حركة الناس والسلع والنقود وجوانب الأمن الالكتروني. وتشارك الولايات المتحدة والشركات الأمريكية الرائدة في هذه المبادرة ولكن من دون نتائج ملموسة.

وفضلا عن الجرائم الالكترونية فان النظام الدولي بحاجة إلى تطوير مفهوم حول ما الذي يؤسس السلام الالكتروني وكذلك ما الذي يمكن أن يشكل سلوكاً معقولاً وما الذي لا يشكل ذلك. وفي المجال العسكري سيحتاج الدبلوماسيون إلى تشكيل أفكار حول الردع والسيطرة على التسلح وبناء الثقة المناسبة لاسيما في مجال الفضاء الالكتروني. وسوف يكون هناك حاجة إلى أداة الخط الساخن الالكتروني بهدف تسريع الاتصالات بين المختصين في تكنولوجيا

المعلومات والاتصالات فيما يتعلق بالهجمات الالكترونية المفترضة من قبل إحدى الدول تجاه الدولة الأخرى.

إن هناك أمثله أخرى في مجال الآمن الالكتروني، إذ أن مستويات التعاون والثقة عالية جداً. ومن ابرز الأمثلة على ذلك هو الذهاب إلى ابعد من النظام الدولي للمستويات المصرفية. ومن الأمثلة الأخرى هي الجرائم الالكترونية والمعايير الدولية للتنمية. ومع ذلك، فان الحكومات لاسيما تلك المهتمة بارتكاب جرائم الآمن الالكتروني لديها ثقة قليلة بان الأدوات الدبلوماسية التقليدية تقدم جزءاً بسيطاً من الحل لهذا التهديد. ويعتقد الكثيرون في روسيا الاتحادية بان الولايات المتحدة تسعى للهيمنة المعلوماتية وإنها تستخدمها في إستراتيجيتها العسكرية مما يجعلها مصدر التهديد الرئيس.

لقد نضجت رؤية اوباما في أيار من العام 2009، وقد دعا فيها الولايات المتحدة إلى تطوير إستراتيجية من اجل تشكيل البيئة الدولية للأمن القومي، وهذا سوف يعني من جملة ما يعنيه بناء تحالفات جديدة مع الدول المتقدمة في المجال التكنولوجي وبضمنها (روسيا الاتحادية، والصين، والهند) بهدف مواجهة التهديدات للاعبين غير حكوميين ودول مارقة. كما انه يجب أن نتوقع بأنه سوف يكون هناك بعض ردات الفعل حول المفهوم الأمني الجديد لحلف شمال الأطلسي الجديد الذي نشر في عام 2010.

وبالنسبة لهذا الأمر، تقود روسيا الاتحادية على مدى أكثر من عقد من الزمان جهوداً حثيثةً في إطار الأمم المتحدة بهدف تأسيس بعض قواعد اللعبة.

وفي عام 1998 وفي أطار الجمعية العامة للأمم المتحدة عملت روسيا الاتحادية على تبني مشروع قرار (لم يتم التصويت عليه) حول التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في إطار الأمن الدولي. وقد نص القرار على ما يأتي :

1- يدعو كل الدول الأعضاء إلى تعزيز المستويات المتعددة مع الأخذ بنظر الاعتبار التهديدات القائمة والمحتملة في مجال الأمن ألمعلوماتي.

2- يدعو كل الدول الأعضاء إلى إعلام الأمين العام بوجهات نظرهم وتقييم المسائل الآتية:

أ - التعليم العام لقضايا الأمن المعلوماتي.

ب - تعريف المفاهيم الأساسية المرتبطة بالأمن المعلوماتي بما في ذلك التدخل بدون أذن مسبق فيما يتعلق بإساءة استخدام المعلومات والاتصالات السلكية واللاسلكية ومصادر المعلومات.

ج - تقديم المشورة فيما يتعلق بتطوير المبادئ الدولية التي سوف تعمل على تحسين امن الأنظمة العالمية للمعلومات والاتصالات السلكية واللاسلكية، كما تساعد على مكافحة الإرهاب المعلوماتي والجريمة المنظمة.

وبحلول عام 2009، بذلت الجمعية العامة للأمم المتحدة لأكثر من عقد من الزمان نشاطا دبلوماسياً عالميا بهدف أعداد مشروع قرار يتعلق بخلق ثقافة

عامة في مجال الأمـن الالكـتروني. وان العلامـة البـارزة تتمثـل في القمـة العالميـة حـول المجتمـع المعلومـاتي مـن خـلال تأسـيس المجموعـة المتقدمـة للخـبراء وتخـتص بـالأمن المعلومـاتي، فـضلا عـن المـنظمات غـير الحكوميـة التـي تعمـل مـن خـلال المـنظمات مثـل فريـق المراقبـة الدائمـة والاتحاد العالمي لأمن المعلومات والشراكة الدولية المتعددة الأطـراف لمكافحـة تهديـدات الأمـن المعلوماتي.

لقد شارك المتخصصون والمسؤولون من الولايـات المتحـدة و روسـيا الاتحاديـة في معظـم المشاورات المتعددة الأطراف ولكن لم يوقع أي منها بوصفه شريكا في (الشراكة الدولية المتعـددة الأطراف ضد تهديدات الأمن المعلوماتي على الرغم من أنهما يتحملان عبء الزعامة العالمية فيما يتعلق بـ (بأمين أسرار الأمن المعلوماتي في الاتحاد الدولي للاتصالات السلكية واللاسلكية).

وعلى الرغم من أن البلدين يـشاركان في مثـل هـذه المبـادرات المتعـددة الأطـراف إلا أن الاتصالات الثنائية كانت ضعيفة بشكل كبير.

وبنهاية عام 2009، عزز مشروع الأمم المتحدة الذي تم تقديمه من قبل روسيا الاتحاديـة من الوسائل المهمة التي تحاكي مخاوف الولايات المتحـدة. وكنتيجـة لـذلك، تـم الموافقـة في تلـك السنة عليه من قبل الجمعية العامة للأمم المتحدة، وقد دعمته الولايات المتحدة. وقد نص هـذا القرار[1] على ما يأتي:

(1) ملاحظة: فيما يتعلق بنص القرار تم الرجوع والاستعانة بالنص الأصلي العربي للقرار لكي تكون الترجمة كـما هي في الوثيقة الرسمية. المترجم.

1- نهيب بالدول الأعضاء أن تواصل تـشجيع النظـر، عـلى الـصعد المتعـددة الأطـراف، في الأخطار القائمة والمحتملة في ميدان امن المعلومات، وكذلك ما يمكن اتخاذه من تدابير للحد من الأخطار التي تنشأ في هذا الميدان، بما يتماشى وضرورة المحافظة على التدفق الحر للمعلومات.

2- ترى انه يمكن تحقيق الغرض من هذه التدابير عـن طريـق دراسـة المفـاهيم الدوليـة ذات الصلة التي تهدف إلى تعزيز امن النظم العالمية للمعلومات والاتصالات الـسلكية واللاسلكية؛

3- تدعو جميع الدول الأعـضاء إلى التواصـل مـع الأمـين العـام بآرائهـا وتقييماتهـا بـشأن المسائل الآتية:

أ- التقييم العام لمسائل امن المعلومات؛

ب- الجهود المبذولة على الصعيد الـوطني لتعزيـز امـن المعلومـات وتـشجيع التعـاون الدولي في هذا الميدان؛

ت- مضمون المفاهيم المذكورة في الفقرة 2 أعلاه.

ث- التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز امن المعلومات على الصعيد العالمي.

4- تطلب إلى الأمـين العـام أن يواصـل، بمـساعدة فريـق الخـبراء الحكـوميين المنـشأ في عـام 2009 اسـتنادا إلى مبـدأ التوزيـع الجغـرافي العـادل عمـلا

بقرار الجمعية العامة 37/63، النظر في الأخطار القائمة والمحتملة في ميدان امن المعلومات وفي التدابير القانونية الممكنة للتصدي لها، وكذلك المفاهيم المشار إليها في الفقرة 2 أعلاه وان يقدم إلى الجمعية العامة في دورتها الخامسة والستين تقريرا على نتائج هذه الدراسة.

5- تلاحظ مع الارتياح عقد الدورة الأولى لفريق الخبراء الحكوميين الذي أنشأه الأمين العام، في جنيف في تشرين الثاني من العام 2009، واعتزام الفريق عقد ثلاث دورات أخرى في عام 2010 للاضطلاع بولايته المنصوص عليها في القرار 37/63.

6- تقرر أن تدرج في جدول الأعمال المؤقت لدورتها الخامسة والستين البند المعنون " التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سباق الأمن الدولي."

مما لاشك فيه أن العمل بين الولايات المتحدة وروسيا الاتحادية في إطار اللغة المقبولة للطرفين فيما يتعلق بقرار الأمم المتحدة قد ساعد بشكل فاعل على تحسين الدبلوماسية الثنائية الالكترونية بين الطرفين. وبحلول تموز من العام 2010، كان هناك مناقشات مستفيضة على المستوى الرسمي بضمنها زيارات المسؤولين رفيعي المستوى من قبل الأمين المساعد لشؤون الاتصالات السلكية واللاسلكية (لورنس) ومنسق سياسة الاتصالات والمعلومات الدولية فضلاً عن السفير فليب ڤيرڤير. لقد حضروا منتدى تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية الأمريكية الروسية. وفي أيار عقد الاجتماع الأول في عام

2004. لقد كان من المفترض أن يعمل المنتدى الثاني على تحفيز الحوار حول مجموعة كبيرة مـن القضايا ومن ضمنها الأمن الالكتروني. ومن بين القضايا الأخرى الرسـائل العـشوائية وإدارة شـبكة المعلومات الدولية والإدارة المتعددة الأطراف لتنسيق البث التلفزيوني الرقمي وتنـسيق المواقـف فيما يتعلق بالاجتماعات القادمة للاتحاد الدولي للاتصالات. لقد التقى وفد الولايات المتحدة مـع ممثلي الصناعة وشارك في الملتقـى الحكـومي الـروسي الأول حـول شـبكة المعلومـات الدوليـة في منتدى البنية التحتية الإستراتيجية الذي عقد برعاية مجلس إدارة الأعمال الروسي الأمريكي. وقـد عمل المسؤولون الأمريكيون على ربط الملتقى باللجنة الرئاسية الثنائية، على الرغم من أن منتدى تكنولوجيا المعلومات والاتصالات ليس واحداً من مجموعات العمل المشكلة رسمياً لتلك اللجنة.

يمكن القول أن هناك مجموعة من السوابق التاريخية الدامغة التي تشير إلى التحفظـات الموجودة في روسيا الاتحادية والولايات المتحدة حول الحساسيات الكبيرة للأمن الوطني المتمثلـة بالتعاون في مجال الأمن الالكتروني وهذه الحساسيات يمكن تجاوزها، إذ كان هناك اعتراض واحد سابقاً يتمثل بعدم السماح لطائرة احد البلدان بالمرور فوق المدن الرئيـسة للبلـد الآخـر. كـما أن الخط الساخن الذي تم إنشاءه من قبل كيندي وخرشوف في عام 1963 هو المثـال البـارز لـذلك. إن التعاون المشترك أسهم في تشكيل المنظمة الحربية للفضاء (وهي منظمة ليس ربحية كما أنها تأسست بناءً على طلب المنظمة الحربية الدولية بهدف أنـشاء شـبكة مـن الاتـصالات الفـضائية للمجتمع الفضائي وتفسيرها.

كما أن هناك قضايا حساسة تتعلق بنقل التكنولوجيا وارتباط مصالح القطاع الخاص فيها بشكل كبير، ولذلك تم وضع آليات عديدة لمواجهة هذه الحاجة. وأثناء عملية الأعداد Y2k، كان هناك تهديد عالمي، لذلك فان معظم البلدان تتعاون على الرغم من حساسيات الأمن القومي. كما تبنت الولايات المتحدة وروسيا الاتحادية تدابير مشتركة في مجال المراقبة المشتركة لمعظم إجراءات الإطلاق والإنذار للصواريخ الباليستية. كما أن هناك قلة وعي عام فيما يتعلق بقيمة السوابق التاريخية، وحتى في حالة إدراكها، كيف يمكن تخطي هذه المعارضة للعمل التعاوني حول الأمن الالكتروني.

انه لأمر مهم للولايات المتحدة وروسيا الاتحادية أن يدرك الطرفان بان الأمن الالكتروني هو مشكلة عالمية تتخطى الحدود الوطنية، كما أن المفهوم التقليدي للقوة الوطنية والذي يرتكز على العناصر الاقتصادية والسياسية والعسكرية ذات تأثير قليل الأهمية في الآمن الالكتروني. وان الطبيعة غير المتكافئة للهجمات الالكترونية يجعل من تشكيل أي سياسة ناجعة أمر صعب جداً. وقد أشار تقرير صدر مؤخراً إلى أن (الحماية الشاملة للبنية التحتية الأساسية بإكمالها ضد كل التهديدات والمخاطر تعد مستحيلة، ليس فقط لأسباب فنية وعملية بل أنها مكلفة بشكل كبير.

أن مسألة الأمن الالكتروني تطرح مشكلة لصناع السياسة تماثل في أهميتها مشكلة الإرهاب. كما أن الطبيعة العالمية لشبكة المعلومات الدولية تعني بان الهجمات يمكن تنفيذها في أي مكان في العالم. وقد ذكرت لجنة مركز الدراسات

الإستراتيجية حول الفضاء الالكتروني ما يأتي (نوصي الولايات المتحدة أن تكرس جهودها وتدابيرها من اجل تامين الفضاء الالكتروني من خلال مبادرة متعددة الأطراف وفي كل مجال يعد مناسباً لذلك، كما ندعو الولايات المتحدة إلى اتخاذ الإجراءات الضرورية بغية تامين القضاء الالكتروني في أي مبادرة متعددة الأطراف حيثما يكون ذلك مناسبا كما نفعل نحن فيما يتعلق باتخاذ الإجراءات من اجل تحقيق التقدم في مجال حضر انتشار الأسلحة النووية ومكافحة الإرهاب.

وعلى العكس من الأعمال الإرهابية، فان الهجمات الالكترونية من الصعب التحقق منها واكتشافها واكتشاف جذورها والهجمات الناتجة منها، (والتي يطلق عليها المشكلة العشوائية) وتعد صعبة بشكل كبير. إذ أن هناك ساحة للمعركة ليس من خلال خط المواجهة الأمامي (أي الالتحام العسكري المباشر)، كما أن معظم ضحايا الهجمات الالكترونية الفردية يمكن أن تنتشر في غضون خمس دقائق وتشمل عشرات الدول. لذلك فالدول وهيئات تنفيذ القانون عجزت مراراً وتكراراً في مواجهة هذه التهديدات الجديدة العابرة للحدود. يمكن القول أن لدى الولايات المتحدة وروسيا الاتحادية الكثير لكي تقوم به من خلال التعاون المتبادل حول الأمن المتبادل. ولقد أشار إلى ذلك ممثل الحكومة الروسية في الجمعية العامة للأمم المتحدة:

"أن الثورة المعلوماتية ظاهرة عالمية تؤثر في كل جوانب المجتمع من مثل المرافق الدولية والجوانب السياسية والاقتصادية والقطاع المالي والعلوم والثقافة. كما أصبحت مصادر المعلومات واحدة من الأصول الوطنية والدولية القيمة. وفي الوقت ذاته فان هناك قلقاً بالغ حول التهديدات المحتملة. ومواجهة ذلك سوف يحقق السلام والاستقرار والأمن الدولي. وعلى هذا الأساس، من المهم الحد من المواجهات الدولية المحتملة ضمن الاتصالات السلكية واللاسلكية الدولية".

المحور الثاني: المنهجين المتناقضين في مجال الأمن الالكتروني

يتركز نهج سياسة الحكومة الروسية في مجال الأمن الالكتروني على أولويات تختلف في مضمونها عن أولويات الولايات المتحدة الأمريكية. إذ طبقا لوجهه نظر الخبراء الروس فان مصطلح الأمن الالكتروني والفضاء الالكتروني في الولايات المتحدة يأخذ في المقام الأول طابعاً تكنولوجياً، بينما تشمل المصطلحات الروسية على مفردات مثل الأمن المعلوماتي والفضاء المعلوماتي ومن ثم فان هذه المصطلحات تنطوي على معاني فلسفية وسياسية وتأخذ بعداً أوسع.

إن التكنولوجيا ينظر إليها في روسيا الاتحادية على أنها واحدة من العناصر الكثيرة المتعلقة بالإدراك الروسي للأمن المعلومات ولكنها لا تعد الشيء الوحيد والمهم بالنسبة لها.

إن عقيدة الأمن المعلوماتي لروسيا الاتحادية على سبيل المثال لا تذكر كلمة انترنت في بطون نصوصها. كما أن الأهداف المعلنة لروسيا الاتحادية في مفهومها للأمن المعلوماتي ترتكز على حماية الثقافة والمعرفة القومية وتتضمن كذلك سهولة الوصول إلى المعلومات.

وبالطبع فان المطالبات الأخيرة الحامية الوطيس من نقاد الكرملين سواءاً كانوا في الداخل أم في الخارج والتي تتعلق باعتقادهم بان مفهوم الأمن المعلوماتي صمم في الحقيقة من اجل إسكات الانتقادات الموجهة ضد الحكومة.

ومما لاشك فيه أن هذا الأمر يعقد الحالة السياسية وعملية صنع القرار لدى المسؤولين في الولايات المتحدة الأمريكية كما أنهم يخشون الانتقادات المحلية في التعاون مع روسيا الاتحادية بهدف تحسين التعاون في مجال الأمن الالكتروني. وتتمثل الأولويات الرئيسة لسياسة الولايات المتحدة في مجال الأمن المعلوماتي في الحفاظ على التكنولوجيا المحلية من التدهور أو الوصول غير المصرح به أو أي نوع آخر من أنواع التدخل مع التأكيد على الجوانب التكنولوجية للأمن الالكتروني.

وعلى العموم، تركز الولايات المتحدة بشكل كبير على منهج تنفيذ القانون المحلي، بينما تفضل روسيا الاتحادية تحقيق هدف آخر يتمثل بتأسيس أنظمة دولية. إن هناك مقبولية لكلا المنهجين لأنهما يكملان بعضهما البعض.

وقد أكد تقرير أصدرته لجنة الدراسات الإستراتيجية والدولية حول الأمن الالكتروني وطبيعة البيئة الرقمية العالمية من أن شبكة المعلومات الدولية هي بمثابة حي من أحياء المدينة إذ يشترك الناس في السياسة والحديث كما أن هناك الشارع الرئيس الذي يتبضع الناس فيه أو في جزء منه، كما أن هناك أزقة مظلمة وهو المكان الذي تحدث فيه الجريمة، وفي جزء منه هناك ممرات سرية يشترك الجواسيس في التجسس الاقتصادي والعسكري وكل ما تقدم هو بمثابة ساحة للمعركة. ولذلك فان سوء التفاهم بين الأطراف الفاعلة آمر لا مفر منه ومن ثم فانه أمر لا يمكن معالجته من دون الحوار والتسوية.

أولا: روسيا الاتحادية:

لقد بدأت روسيا الاتحادية منذ وقت طويل في التركيز على العناصر الرئيسة للآثار المترتبة على الأمن الالكتروني. لذلك تم مناقشة هذا الموضوع مناقشة حامية الوطيس عندما تـم تأسـيس مجلس الأمن القومي الروسي في عام 1992. إن المنظمات والهيئات المسؤولة عن الأمن الالكتروني في روسيا الاتحادية هي مجلس الأمن القـومي الـروسي وجهـاز الأمـن الاتحـادي (أف أس بي كـما يسمى في روسيا الاتحادية) وجهاز الحـرس الاتحـادي ووزارة تكنولوجيـا المعلومـات والاتـصالات السلكية واللاسلكية.

إن هناك فصلاً كبيراً للمسؤوليات عندما يتعلق بالنشاطات المرتبطة بالجانـب الالكـتروني في الحكومة الروسية وهي كما يأتي :

- وزارة الـشؤون الداخليـة (والتـي تعـرف في روسـيا الاتحاديـة اختـصاراً بـ MVD): هــي المسؤولة عن مكافحة الجريمة الالكترونية.
- وزارة الدفاع: هي الوزارة المسؤولة عن الحرب الالكترونية.
- جهاز الأمن الاتحادي: هو الجهاز المسؤول عن مكافحة الإرهـاب الالكـتروني. وجوانـب أخرى تتمثل في السيطرة عن الأمن الداخلي والدولة.

إن هذا الجهاز وبالتعاون مع الحكومة الروسية يؤكد أن المجالات الرئيسة تتمثل في الجريمة والإرهاب والتهديدات العسكرية والسياسية في مجالات الأمن الالكتروني. كما يتم تنسيق السياسة الروسية من خلال لجنة تتولى التنسيق بين الهيئات في مجلس الأمن القومي الروسي الذي يترأسه فلاذ أسلافا شيرستول والأمين المساعد في المجلس هو بور بيس ماشتكوف رئيس مكتب مكافحة الجرائم التكنولوجية المتقدمة وهو تابع لوزارة الشؤون الداخلية.

إن عقيدة الأمن المعلوماتي الروسية التي تم تبنيها في أيلول من العام 2000 تعرف الأمن المعلوماتي بأنه (حماية المصلحة الوطنية الروسية في مجال الأمن ألمعلوماتي)، التي حددت بدورها مجمل المصالح المتوازنة للأفراد والمجتمع والدولة. كما انه يتعامل مع مجموعة واسعة من القضايا بدءاً من حماية البيانات والخصوصية الشخصية وقرصنة أسرار الدولة وعملية الوصول إلى المعلومات.

وطبقاً لتقرير صدر مؤخراً فان الغرض الرئيس من السياسة المعلوماتية الروسية هو المساهمة في استقرار التنمية الاجتماعية والسياسية داخل روسيا الاتحادية وضمان الدعم الشعبي للسياسات الروسية الرسمية.

لقد حددت الحكومة الروسية عام 2010 أربعة أهداف مركزية تتعلق بسياسة الدولة في مجال الأمن المعلوماتي وهي كما يأتي :

1- تطوير النظم القيمية للمجتمع الروسي

2- ضمان الدعم لنشاطات الدولة من قبل الرأي العام الوطني والمحلي (الدعم الشعبي لسياسة الدولة).

3- مكافحة الإيديولوجيات الهدامة والتطرف الديني وتضليل المؤسسات الدولية والوطنية حول سياسات الدولة وتحديداً في الجوانب المتعلقة بالمعلومات السياسية.

4- مواجهة الحالة المتدهورة للأمن والاستقرار وتفعيل بنية الدولة الوطنية وبضمنها الجوانب العسكرية والتكنولوجية والسياسية.

ترى روسيا الاتحادية ونتيجة تصورها حول نقص تكنولوجيا الاتصالات ضرورة عقد معاهدة دولية تأخذ على عاتقها عملية حظر أو منع تطوير أو استخدام مجالات واسعة من تكنولوجيا المعلومات المدنية والعسكرية. وتكمن الرؤية الروسية حول هذه الاتفاقية في أنها يجب أن تعالج بشكل محدد تهديدات الهجمات الالكترونية، كما إنها تعالج سباق التسلح الرقمي، علاوة على ما تقدم فانه يجب أن تتضمن هذه الاتفاقية تعريفات مقررة ومعترف بها من قبل المجتمع الدولي حول الفضاء الالكتروني والأسلحة المعلوماتية. وطبقاً لتقرير صدر مؤخراً حول البنية التحتية الأساسية الروسية، فان العقلانية في تعزيز هذه المسائل تعد مصلحة وطنية (أي إن المنطق العقلاني والمصلحة الوطنية تمكن في التوصل إلى عقد مثل هذه المعاهدة والاتفاقية).

إن التعاون الدولي لروسيا الاتحادية في مجال تامين الأمن المعلوماتي له ميزتان: لقد زاد التنافس الدولي من اجل الحصول على المصادر التكنولوجية والمعلوماتية والهيمنة على الأسواق يوماً بعد يوم. كما إن الاقتصاديات العالمية الرائدة حققت نمواً مضطردا في مجال التكنولوجيا وأدت إلى السماح لهم لبناء إمكانياتهم في مجال الحرب الالكترونية. لذلك فان روسيا الاتحادية تراقب هذا التطور مع قلق بالغ، إذ أن ذلك من الممكن أن يؤدي إلى سباق تسلح جديد في المجال المعلوماتي ويزيد من مستوى تهديد أجهزة المخابرات الخارجية ومن ثم يسهم في اختراق البنية التحتية المعلوماتية الدولية لروسيا الاتحادية عن طريق الوسائل التقنية.

وعلى هذا الأساس، ترغب روسيا الاتحادية بشكل كبير وضع قيداً على الأسلحة الالكترونية الهجومية. وممكن أن يتم ذلك عن طريق معاهداتها المقترحة التي سوف تحظر بدورها (الأسلحة الهجومية) مثل حظر الرموز والبرمجيات الخبيثة التي يمكن تفعيلها عند بدء الحرب، ومما لاشك فيه تقدم المقترحات الروسية فكرة واضحة عن توسيع حق الحكومات في تقييد أو منع نقل المعلومات إلى داخل الحدود الوطنية من خارج الحدود التي ربما تسبب تعطيلاً سياسياً واجتماعياً وثقافياً.

وبهدف مضي روسيا الاتحادية في أجندتها في مجال الأمن الالكتروني فأنها طبقا لقرار الجمعية العامة للأمم المتحدة ذي الرقم 32/58 ترأست مجموعة العمل للخبراء الحكوميين التابعة للأمم المتحدة حول الأمن الالكتروني في عام

2003، وقد استمرت في ممارسة دور قيادي في مجموعة خبراء شبيهة حتى عام 2010. فضلا عن ذلك فقد أسست روسيا الاتحادية شركات خاصة حول الأمن المعلوماتي مع أعضاء منظمة شنغهاي للتعاون ومنظمة الأمن الجماعي.

وطبقاً لوجهة نظر المسؤولين الروس الكبار فان التطور البالغ الأهمية يتمثل في تبني منظمة شنغهاي للتعاون معاهدة حول الأمن المعلوماتي عام 2009، وتهدف المعاهدة إلى وضع أساس سياسي وقانوني ومؤسساتي يهدف إلى تعزيز الثقة وتطوير التعاون بين كل الأطراف والوكالات الوطنية ذات العلاقة.

ثانيا: الولايات المتحدة الأمريكية

لقد عينت إدارة اوباما في عام 2009 منسقا للأمن الالكتروني كجزء من هيئة الأمن القومي بهدف العمل على تنسيق الإستراتيجية القومية في هذا المجال. ويقع على عاتق المنصب الجديد مهمة تقديم سياسة قومية متماسكة بهدف تعزيز وتحسين الدفاع الالكتروني للبنية التحتية الأساسية فضلاً عن تنسيق نشاط الحكومة الاتحادية في مجال الأمن الالكتروني.

لقد كان هناك العديد من المبادرات والسياسات في الماضي تتعلق بمجال الأمن الالكتروني مثل الإستراتيجية القومية لتأمين الفضاء الالكتروني لعام 2000، وخطة حماية البنية التحتية القومية لعام 2006، والإستراتيجية القومية للتشارك المعلوماتي لعام 2007، وفي كانون الثاني من عام 2008، أعدت إدارة الرئيس بوش المبادرة الشاملة للأمن الالكتروني القومي بهدف جعل الولايات

المتحدة أكثر أمنا ضد التهديدات الالكترونية. وقد كانت الأوامر التي أوجدت هذه المبادرة سرية للغاية.

أن المنظمات والوكالات التي تتعامل مع قضايا الأمن المعلوماتي في الحكومة الاتحادية هي وزارة الأمن الوطني، ووزارة الخارجية ووزارة الدفاع ومكتب الأمن المعلوماتي ووزارة الاتصالات السلكية واللاسلكية والأمن الالكتروني ومركز حماية الأمن الالكتروني الوطني وقسم جرائم الحاسوب والملكية الفكرية في وزارة العدل.

كما تدعم الولايات المتحدة المنهج الدفاعي الذي يقوم على أن التعاون المستمر على تنفيذ القانون الدولي يعد عنصراً مركزياً. علاوة على ذلك، ترى الولايات المتحدة بان هدف الأمن الالكتروني يمكن تحقيقه من خلال مركزية الدولة، إذ أن الدولة تعمل على المستوى الوطني وتتعاون على المستوى الدولي بهدف تحسين وصيانة امن بنيتها التحتية الأساسية، فعلى سبيل المثال، وطبقاً لورقة العمل التي قدمتها الولايات المتحدة إلى القمة العالمية حول مجتمع المعلومات في عام 2003، ومن خلال خطة العمل هذه دعمت الولايات المتحدة الفكرة التي ترتكز على أن كل دولة يجب أن تضع برنامجاً وطنياً يرتكز على ما يأتي:

1- تثقيف وتعزيز الوعي لأفضل الممارسات في شبكة المعلومات وامن البنية التحتية.

2- تجريم سوء استخدام تكنولوجيا المعلومات بشكل فاعل.

3- تبني شراكة متقدمة بين الحكومة والمجتمع الصناعي بهدف تقديم حافز يعمل على ضمان الأمن لأنظمتهم القومية.

4- تأسيس الإجراءات وقدرات التحذير والاستجابة للحوادث الوطنية من اجل المشاركة الشاملة في مجال المعلومات وطنيا ودوليا.

وفيما يتعلق بالمعايير الدولية والتعاون فان وجهة نظر الإدارة الحالية للولايات المتحدة حول سياسة الفضاء الالكتروني تتضمن ما يأتي:

"إن المعايير الدولية كفيلة بتأسيس بنية تحتية رقميه آمنة ومستقرة. فضلا عن ذلك فان الاختلاف في القوانين الوطنية والإقليمية وتطبيقاتها مثل (القوانين المتعلقة بالتحقيق والمرافعة حول الجريمة الالكترونية وحفظ البيانات والحماية والخصوصية وطرق الدفاع عن الشبكة ومواجهة الهجمات الالكترونية) يشكل تحديا خطراً في الوقت الحاضر فيما يتعلق بتحقيق بيئة رقمية سليمة وأمنية وهادئة. لذلك فان العمل مع الشركاء الدوليين هو السبيل الذي يمكن من خلاله أن تعالج الولايات المتحدة بشكل فاعل هذه المنافع المترتبة على العصر الرقمي".

وكما يوضح الاقتباس أعلاه, فان الولايات المتحدة كما هو حال روسيا الاتحادية تعتقد بان التهديد الرئيس للأمن الالكتروني ينبع من الجريمة المنظمة وقارضة الحواسيب الالكترونية واللاعبين غير الحكوميين ومن ضمنهم الإرهاب. وهذا ما أكدته ورقة الولايات المتحدة المقدمة إلى القمة العالمية عام 2003 السالفة الذكر. وهذا ما تم تأكيده من قبل الورقة التي قدمت القمة العالمية حول خطة عمل المجتمع ألمعلوماتي:

"إن منافع الفضاء الالكتروني يمكن حمايتها بشكل أفضل من خلال التركيـز عـلى التجـريم الواضح للدول التي تسيء استخدام تكنولوجيا المعلومات والتنفيذ الوطني المـنظم للتـدابير التـي صممت لمنع الأضرار التي تؤذي البنية التحتية الأساسية بغض النظر عن مصادر التهديد، وان مـا تدعو إليه الولايات المتحدة هو خلق ثقافة عالمية عن الأمن المعلوماتي".

لقد عارضت الولايات المتحدة وضع "(قيود للأمن الالكتروني)"، وهو المـنهج الـذي تؤيـده روسيا الاتحادية، وترى بان ذلك هو التحدي المباشر للمبادئ الديمقراطية التي يمكن أن تستخدم بسهولة من قبل الحكومات من اجل تبرير القيود المفروضة عـلى حريـة الوصـول إلى المعلومـات والاستخدام السلمي لتكنولوجيا المعلومات.

لقد أكد المسؤولون الأمريكيون في عدد من البيانات المتعلقة بالأمن الالكتروني على حرية الأفراد في البحث عن المعلومات والأفكار واستقبالها وإرسـالها طبقـاً للـمادة التاسـعة عـشر مـن الإعلان العالمي لحقوق الإنسان.

وعلى الرغم من الجهود الحالية والماضـية حـول القـضايا الالكترونيـة، فـان تقريـرا صـدر مؤخراً حول الانغماس الأمريكي الدولي في مجال الأمن الالكتروني وجد بان الجوانب الدولية للأمن الالكتروني تعد من اقل العناصر ايلاءاً للأهمية في سياسة الولايات المتحدة الأمريكية.

إن الجوانـب الدوليـة والعالميـة المتعـددة الأطـراف لأمـن شـبكة المعلومـات الدولية لابد أن يتم إدراكهـا بوصـفها قـضية مترابطـة بـشكل كبـير التـي يمكـن مـن

خلالها تعزيز المنافع التي تعزز أهداف الولايات المتحدة الأمريكيـة وفي الوقـت ذاتـه تقلـل مـن المخاطر.

وعلى الرغم من أن الخبراء حذروا من التحريض ضد القلق الالكتروني مـن خـلال تـصاعد التهديدات الالكترونية، فانه لـيس هنـاك شـك بـان زيـادة عـدد الهجـمات الالكترونيـة وتطـوير منهجياتها يتطلب منهجيات سياسية جديـدة. لقـد ذكـر مـدير وكالـة المخـابرات القوميـة مـيكي ميكوثيال بان الوقت ليس طويلاً عندما يصل مستوى التطـور إلى النقطـة التـي مـن الممكـن أن تشكل تهديداً استراتيجياً للولايات المتحدة الأمريكية.

فضلا عن ذلك، لقد بقيت الولايات المتحدة ينتابها الشكك تجاه الأفكـار الروسـية لاسـيما فيما يتعلق بالاتفاقية الدولية لان ذلك يمكن أن يـوفر غطـاءً للأنظمـة الـشمولية لمراقبـة شـبكة المعلومات الدولية. كما أن الولايات المتحدة قلقة من أن الاتفاقية ربما تكون غير فاعلة لأنـه مـن المستحيل الآن تحديد فيما إذا كانت الهجمات على شبكة المعلومات الدولية نابعة من الحكومـة أو القراصنة الموالين لتلك الحكومة أو عن طريق الدول المارقة بشكل منفرد.

ومع ذلك، فان الولايـات المتحـدة وافقـت مـؤخراً عـلى البـدء بمحادثـات في لجنة نزع السلاح والأمن الدولي التابعة للأمم المتحـدة بهـدف تعزيـز امـن شـبكة المعلومات الدولية والحد من الاستخدام العسكري للفضاء الالكتروني، إن هذا يعـد تحولاً رئيساً في سياسة الولايات المتحدة الأمريكية بعـد رفـض المقترحـات الروسـية حـول هـذه المبـادرة لـسنوات عديـدة، كـما أن تعيـين منـسق ومستـشار للأمـن

الالكتروني من رئيس الولايات المتحدة في عام 2009 يعد تحـولا نوعيـا. وعـلى هـذا الأسـاس فـان مشروع الاتفاقية المطروحة من قبل الحكومـة الروسـية حـول البروتوكـولات الدوليـة التـي تقيـد استخدام الحرب الالكترونية ليست خارج هذا الإطار. وقد بـدأت محادثـات مبكـرة بـين مجلـس الأمن القومي الروسي وجهاز الأمن الفيدرالي من جهـة ومركـز جـورج مارشـال الأوربي للدراسـات الأمنية عن الجانب الأمريكي.

المحور الثالث: ما الذي يمكن توقعه

يمكن القول أن الولايات المتحدة وروسيا الاتحادية من المحتمل أنهما اشتركتا بشكل روتيني فيما يتعلق بالهجمات والتحقيقات الالكترونية على البنية التحتية الأمنية للدول الأخرى. ولكن مع مرور الوقت، ومع تصاعد وتيرة التقدم التكنولوجي وانتشار الطاقة النووية السلمية، فان بلداناً مثل الولايات المتحدة وروسيا الاتحادية سوف لن ينظر إليهما على أنهما أعداء في مجال الحرب الالكترونية بل على العكس من ذلك كشركاء مهمين بل ربما يصبحوا حلفاء فاعلين.

إن هذا الأمر ربما يستغرق عشر سنوات أو أكثر ولكن المدة الطويلة الأمد تبدو أكثر وضوحاً، إذ أن هناك سوابق تاريخية مهمة مع روسيا الاتحادية. وكما أشار كبار مسؤولي الدفاع في الولايات المتحدة فان الولايات المتحدة وروسيا الاتحادية تتعاونان بشكل هادئ في مركز (Y2K) للاستقرار الاستراتيجي في سبرتك كولورادو، كولورادو في الألفية Rollover. وقد أدى هذا الأمر إلى التشارك في مجال جهود الإنذار المبكر مع روسيا الاتحادية حول إطلاق الصواريخ الطويلة المدى بشكل واسع النطاق على الرغم من كونها قصيرة الأجل ومحددة.

وستكون المخرجات الأولية غير ملموسة ولكنها مع ذلك سوف تكون حساسة في العلاقات الثنائية بين البلدين، وكما اطر الزميل البارز كارل و راسير فأنهم يرشدون البلدان باتجاه بناء الثقة المتقدمة وتشجيع الشفافية.

حيثما يكون مناسباً تقاسم الشعور بالمنفعة المتبادلة والبدء بمناقشة النقاط الجوهرية، ويجب أن لا نعول كثيراً على الثقة ما لم نراها كالتزام مشترك. كما أن التعاون بين الطرفين ممكن، والمشاكل يمكن أن يتم حلها عن طريق المفاوضات. ان مفتاح النجاح الأساسي يمكن من خلاله أجراء حوار ثنائي مع التركيز على نقاط الضعف المتأصلة في المجال الالكتروني بدلاً من تهديدات محددة والتي غالباً ما تكون حساسة.

إن القيمة الطويلة الأمد سوف تتضمن المنافع المحلية الملموسة الآتية:

1- تحسين نوعية الاتصالات الموجودة (تحسين الأمن بشكل أسرع وأكثر مرونة).

2- تطوير القدرات الجديدة بشكل مشترك من اجل تحقيق المنفعة المتبادلة.

3- تجنب التكلفة (الناجمة عن الجريمة، وإعادة توجيه الاستثمار، والفشل في البنية التحتية).

نرى بان الأجندة الواسعة للدولتين حول معالجة الأمن الالكتروني تتضمن القضايا الآتية:

1- **الهويات الموثوق بها** : تطوير منتدى ثنائي يضم القطاعين العام والخاص من اجل مناقشة القضايا المتعلقة بتصديق الشهادات والتوثيق والمجالات الأخرى للبنية التحتية الأمنية والمدنية.

2- **شبكات التحذير المتعلقة بالطوارئ:** ما هـو المـنهج الحـاكم للبلـدان التـي تهـدف إلى تطـوير شـبكات الإنـذار إذا مـا أخـذنا بنظـر الاعتبـار نقـاط الـضعف الالكـتروني والتهديـدات والحوادث.

3- **رفع حالة التوعية:** ما هو المنهج الأفـضل لرفـع حالـة الـوعي مـن اجـل تـسهيل فهـم أصحاب القرار لطبيعة وتوسيع بنيتهم التحتية المعلوماتية الحساسة، وما هو الـدور الـذي يمكـن أن تلعبه كل الأطراف بهدف حمايتهم.

4- **تقييم التهديدات:** هل يوجد ترابط بين البنيـة التحتيـة وكيـف يمكـن تحـسين حمايـة البنية التحتية.

5- **الشراكة بين القطاعين العـام والخـاص** : مـا هـو المـنهج الأفـضل لتعزيـز الـشراكة بـين الأطراف ذات العلاقة سواء في القطاع العام أم الخاص من اجل مشاركة وتحليل معلومات البنيـة التحتية الأساسية بهدف منع الهجمات والتحقق من مواجهة الهجمات على البنية التحتية.

6- **شبكة الاتصالات السلكية واللاسـلكية اللازمـة:** مـا هـو المـنهج الأفـضل لخلـق شـبكة اتصالات سلكية ولاسلكية في أوقات الأزمات واختبارها بهـدف ضـمان بقائهـا آمنـة ومـستقرة في حالات الطوارئ.

7- **متابعـة الهجـمات:** مـا هـو المـنهج الأفـضل لتعقـب الهجـمات عـلى البنيـة التحتيـة المعلوماتية، وكيف يمكن أن نسهل عملية تعقب إفشاء المعلومات بين البلدين.

8- **تداول المعلومات غير قانونية والخطرة:** إن مواقع الانترنت هـي أدوات مثاليـة للنـشر الأفضل وللتضليل على النطاق العالمي. إن المجموعات الإرهابية تـستخدم بـشكل متزايـد شـبكة المعلومات الدولية لعملياتها الدعائية فضلاً عن استخدامها لتجنيد المتطوعين. كـما أصـبح البريـد الالكـتروني واحـدا مـن الأشـكال المهمـة للاتـصال في العـالم. عـلاوة عـلى أن الإرهـابيين يمكـن أن يـستفادوا مـن المنـافع المتمثلـة بعـدم الكـشف عـن الهويـة وسـهولة الوصـول إليهـا في الفـضاء الالكتروني، لذلك كيف يمكن للقطاع العام والخـاص أن يتعاونـا مـن اجـل منـع اسـتخدام شـبكة المعلومات الدولية للأغراض الإرهابية.

المحور الرابع: التدابير العلمية الأربعة المهمة

يقدم هذا الجزء من الدراسة مناقشات مستفيضة بهدف تحقيق تقدم سريع في مجال الدبلوماسية الأمريكية الروسية فيما يتعلق بالأمن ألمعلوماتي (كما يفضل الروس أن يطلقوا عليه) أو الأمن الالكتروني (كما يفضل الأمريكان تسميته). كما تحدد الدراسة بعض الاعتبارات العامة بغية تعزيز المناهج التعاونية لحل المشاكل استناداً إلى الإعلان العام الذي أصدره الطرفان في كانون الأول 2009 الذي تضمن بان يبدأ البلدان مشاورات جديدة في مجال الأمن الالكتروني في إطار الأمم المتحدة. لذلك تناقش الدراسة مجالات التعاون الأربعة الممكنة : البنية التحتية الأساسية العامة، والاستجابة السريعة للجريمة الالكترونية، ومنظمة الأمن والتعاون الأوربية (المعاهد الالكترونية)، والتعاون بين روسيا الاتحادية ومنظمة حلف شمال الأطلسي في مجال الأمن الالكتروني.

إن المجالات الأربعة المقترحة للتعاون بين الولايات المتحدة وروسيا الاتحادية تمثل أفكاراً مجردة لصناع السياسة ولا تتناول التفاصيل الفنية أو الإجراءات التنظيمية لتنفيذها. كما يتضمن المنهج مبادرة إرادية من الولايات المتحدة وروسيا الاتحادية بهدف تقديم مقترح مشترك (لمبادرة) في منتدى دولي (الاتحاد الدولي للاتصالات السلكية واللاسلكية) من اجل ترؤس مجموعات العمل وإشراك الأطراف الأخرى ذات العلاقة في المناقشات. وينبغي أن يعقب ذلك مناقشات ثنائية حول جوانب محددة للتعاون والمجالات الحساسة يمكن أن تناقش في المنتدى الدولي.

المحور الخامس: تكنولوجيا البنية التحتية الرئيسة العامة

إن روسيا الاتحادية تبحث عن منهج جديد في هذا الإطار. وكما أشار احد المتخصصين " نحن نريد مركزاً للثقة من اجل التعامل مع الرسائل العشوائية، وبدون ذلك فان أي تقدم في مجال البنية التحتية الأساسية العامة سوف يكون مستحيلاً. إن زيادة الخبرة في مجال الجريمة الالكترونية والإرهاب الالكتروني والحواجز القليلة أمام المجرمين في الكشف عن هوياتهم، كل ذلك يشير إلى الحاجة إلى العمل من الولايات المتحدة وروسيا الاتحادية. هناك مفارقة واضحة طبقاً للخبراء الروس وهي انه كلما زادت الثقة زادت الجرائم الالكترونية. لقد كان هناك أكثر من 17،000 حالة سجلت في مجال الجريمة الالكترونية في روسيا الاتحادية وحدها في العام 2009. لقد حددت وثيقة سياسية تم الكشف عنها مؤخراً من قبل حكومة الولايات المتحدة الأمريكية الحاجة إلى خلق نظام للثقة حول احد المواضع المرتبطة بالبنية التحتية الأساسية العامة. لقد ركزت الوثيقة على النظام الوطني ولم تعالج الحالات الدولية وحاولت مراقبة جودة الإشراف غير الموضوعي من خلال التركيز على انه كان من المحتمل استخلاصها بين الطرفين. إن الركيزة المهمة تتمثل في أن الاعتماد المتبادل في مجال الفضاء الالكتروني ليس مقتصراً على نظام الثقة القومي.

لقد تم تقديم مفهوم البنية التحتية الأساسية العامة في منتصف عام 1970 وقد شكل تطوراً جديداً في مجال نظام التشفير. وقد سمح هذا النظام للأطراف بتبادل البيانات المشفرة دون التشارك في الأسرار الأساسية مسبقاً. أن السمة

المهمة في نظام التشفير الأساسي العـام تتمثـل بـالتوقيع الالكـتروني الرقمـي وهـو يـشبه التوقيـع المكتوب بخط اليد والذي يمكن استخدامه للتحقق من صحة البيانات أو صحة البيانات المرسلة.

تعد البنيـة التحتيـة الأساسـية واحـدة مـن الاسـتراتيجيات الحيويـة في مكافحـة الجريمـة الالكترونية (مثل سرقة الهوية الشخصية). وذلـك لأنهـا تعـد إحـدى الطـرق البـسيطة في كـشف النقاب عن منتحلي الهويات (مشكلة العشوائية) في المجال الرقمـي. ولكنهـا مـع ذلـك تعـد مـن القضايا الصعبة الحل من خلال مكافحة الجريمة الالكترونية والإرهاب الالكتروني بسبب اخـتلاف المخاوف لدى الولايات المتحدة وروسيا الاتحادية.

لقد نص تقرير أصدره مركز الدراسات الإستراتيجية والدولية بـشكل قـاطع عـلى مـا يـأتي (يجب أن تكون عملية خلق القدرة على المعرفة الموثقة حول من هو الـشخص أو الجهـاز الـذي يقوم بإرسال البيانات المتدفقـة في مجـال الفـضاء الالكـتروني يجـب أن تكـون جـزءاً رئيـسياً مـن إستراتيجية الأمن الالكتروني الفاعلة.

تعد البنية التحتية الأساسية العامة لـوزارة الـدفاع الأمريكيـة الأكـبر في العـالم ومـن ثـم هـي واحـدة مـن أكـثر البنـى تعرضـاً بـشكل واسـع النطـاق للهجـمات الالكترونية. كما أن معظم هذه الهجمات من المستحيل تتبعهـا واقتفـاء أثرهـا وهـو أمر يرجع إلى فقدان التماسك والتناسق في منهجيات التوزيع المتماسـكة. ومـع ذلـك فـان تكـرار الهجـمات الالكترونيـة انخفـض بنـسبة 50% منـذ أن اتخـذ القـسم

قراراً بإدخال نظام الهوية الجديد (بطاقة الوصول إلى البيانات) التـي تعـالج مـشكلة التوزيـع في عام 2008.

وفي دراسة قام بها الاتحاد العالمي لعلماء الرصد والمراقبة الدائمة للأمن الالكتروني تناولت المـشاكل الأساسـية للأمـن الالكـتروني ذكـرت (المـشكلة العـشوائية عـدة مـرات). وقـد تـضمنت توصياتها التي تهدف إلى تحسين الأمن الالكتروني في هذا المجال المحدد ما يأتي:

1- تدعيم إدارة المعلومات على مستوى بنية البيانات بشكل خاص هياكل البيانات المعرفة التي تهدف إلى ضمان تحديد الهوية والتصديق والترخيص للاتصالات مـن اجـل تـأمين الوصول السهل للمعلومات وتأمين إدارة المعلومات عـلى أسـاس القاعـدة الآمنـة التـي تتعلق بتحديد البنية التحتية الأساسية العامة الحالية.

2- تحسين القدرة على تتبع وتحسين وتعقب الاتصالات الالكترونية بهـدف ضـمان مـصدر وهوية من قام بالفعل (التمكن من تحديد المصدر) واستخدام البيانـات الرقميـة عـن طريق الوسائل الفنية والتخفيض الذي يرتكز على التعاون بين مجهزي خدمة الانترنت وفي الوقت ذاته المحافظة على الخصوصية.

3- تطـوير الأدوات التـي تحمـي الخـصوصية وضـمان القـدرة عـلى تـدقيق النشاطات في المجالات التـي تنطـوي عـلى اسـتخدام البيانـات والمراقبـة

الرقمية وصفحات الخدمات الشخصية وحماية البيانات التجارية والشخصية.

4- تطوير آليات تشخص الهويات الرقمية لحماية وتحسين الترابط بين الأجهزة والمعومات والشبكات وتطوير إطار تحديد الهويات التي تحدد المستخدمين الشخصيين واستخدامهم للأجهزة المرتبطة بالشبكة.

5- التأكيد العالي على مكانة التشفير لاسيما من خلال تطوير خوارزميات للتشفير التي لها القدرة على مواجهة تحديات مستقلة وخاصة تلك التي تم تحديدها في الحاسبات التي تستخدم الطاقة (Quantum).

وعلى الرغم من هذه التوصيات، فان هناك القليل من التعاون في مجال البنية التحتية الأساسية بين الولايات المتحدة وروسيا الاتحادية بصرف النظر عن تمويل شركات القطاع الخاص وقطاع الخدمات اللوجستية الالكترونية. وعلى الرغم من أن روسيا الاتحادية دفعت باتجاه تعاون وثيق في هذا المجال لبعض الوقت فأن الولايات المتحدة الأمريكية بقيت حذرة وتخشى بأن التقدم في هذا المجال ربما يستخدم من السلطات الروسية بهدف اتخاذ إجراءات صارمة ضد المنتقدين والمنشقين على النظام.

ومع ذلك، فان بعض المسؤولين الأمريكيين اعدوا مناهج متشابهة للمنهج الروسي. وفي تموز من العام 2009، ذكر روبرت لينز الأمين العام المساعد لوزارة الدفاع لشؤون الهوية الالكترونية والأمن الالكتروني بان انتحال الصفة الشخصية وعدم الكشف عن اسم السارق تعد جوهر العلمية الأمنية على

الانترنت. وقد دعا إلى تأسس ما يسمى (الإمبراطور الالكتروني) من اجل تحديد الهوية والتأكيد على أن تخفيض الإزعاجات تعد مسالة مهمة بهدف ضمان امن ومرونة شبكة المعلومات الدولية. كما أصدرت الولايات المتحدة الأمريكية في وقت لاحق دراسة بعنوان: الإستراتيجية القومية للهويات الموثوقة في الفضاء الالكتروني.

إن جهاز الأمن الاتحادي لروسيا الاتحادية هو الوكالة الروسية الرائدة في مجال التعامل مع مسألة التشفير والتوثيق الرقمي وحماية البنية التحتية الأساسية العامة. كما يجب على لجنة جهاز الأمن الاتحادي إن توافق على جميع الصادرات والاستيرادات المتعلقة بتكنولوجيا التشفير الأجنبية المهمة أو أي تكنولوجيا محلية يتم استيرادها من روسيا الاتحادية. إن أي مناقشات حول التعاون الدولي في مجال البنية التحتية الأساسية العامة يجب أن تبدأ من هذه النقطة.

فعلى سبيل المثال، ممكن أن يدخل مكتب التحقيقات الفدرالي الأمريكي وجهاز امن الاتحاد الروسي في مناقشات حول البنية التحتية الأساسية العامة وتركز على السبل الكفيلة بتحقيق نوع من التوافق بين مجموعة التشفيرات الروسية ونظام ومعايير تشفير البيانات للولايات المتحدة من اجل تحديد نقاط الضعف التي يمكن للأطراف الثالثة مثل المجرمين الإلكترونيين أو الإرهابيين الالكترونيين استغلاها.

وفي روسيا الاتحادية، تعد الجمعية الروسية لشبكات الانترنت والخدمات هي المسؤولة عن تطوير المعايير والوثائق القانونية المتعلقة بتنفيذ والاستخدام

الأمن للبنية التحتية للاتصالات السلكية واللاسلكية الدولية. وقد تأسست من خلال مبادرة قدمتها وزارة تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية الروسية في عام 1994. وفي الوقت الحاضر تملك الجمعية الروسية لشبكات الانترنت والخدمات أكثر من 110 عضواً من روسيا الاتحادية كلها وبضمنها الجامعات والمؤسسات العلمية والوزارات.

إن الجمعية الروسية لشبكات الانترنت والخدمات لها العديد من اللجان ومجموعات العمل حول العديد من الموضوعات مثل الانترنت والأمن الخصوصية والاتصالات السلكية واللاسلكية ومن خلال الأمن لمعلوماتي تتعامل الجمعية الروسية لشبكات الانترنت والخدمات على إنشاء البنية التحتية العامة وتطويرها، ومفهوم الأمن المعلوماتي في روسيا الاتحادية، وأعداد مشروعات القوانين المتعلقة بالتواقيع الالكترونية، وتكامل أنظمة المعلومات والاتصالات السلكية واللاسلكية الروسية مع البنية التحتية الأوربية والعالمية.

وبسبب الأهمية البالغة للقطاع الخاص في تطوير منتجات التشفير مثل التواقيع الالكترونية، فان شراكة بين القطاعين العام والخاص سوف تكون مهمة بشكل كبير. إن معظم البنية التحتية الأساسية في الطاقة والاتصالات السلكية واللاسلكية والتنقل والخدمات المالية في كلا البلدين مسيطر عليه من القطاع الخاص. ويمكن وضع حوافز للتعاون بين القطاع الخاص ذاته في مجال تكنولوجيا التشفير، إذ تقوم الشركة الأمريكية بتطوير الأجهزة الصلبة للحاسوب بينما تقوم الشركة الروسية بتطوير الأجهزة المرنة للحاسوب. إن هناك خيارات مهمة فيما

يتعلق بالمنتجات المتعلقة بالتشفير والطرق التي تفي بمتطلباتها والتي تتم من خلال جهود مشتركة بين الولايات المتحدة وروسيا الاتحادية في هذا المجال، كما يمكن لكيان محايد متعدد الأطراف (مركز الثقة كما وصفه الخبراء الروس مؤخراً) أن يقدم مشورة سياسية وفنية غير حزبية لكلتا الحكومتين والدول الأخرى الرائدة في مجال الالكتروني.

إن الاتحاد الدولي للاتصالات السلكية واللاسلكية تقع على عاتقه المسؤولية الكاملة عن الجوانب العملية ومؤثرات الأمن الالكتروني الدولي، كما إن الاتحاد يمكن أن يكون المنظمة المناسبة لدعم المبادرة الفنية المشتركة الأولى لروسيا الاتحادية والولايات المتحدة حول البنية التحتية الأساسية العامة. لقد طور الاتحاد الدولي للاتصالات السلكية واللاسلكية معياراً دولياً للبنية التحتية الأساسية العامة. (التي تسمى ((ITU × 509,)) كما أنها تعرف اختصاراً (- ISO 9494808).

لقد دعمت الولايات المتحدة وروسيا الاتحادية أجندة الأمن الالكتروني العالمي التي أطلقها الاتحاد الدولي للاتصالات السلكية واللاسلكية في أيار من لعام 2007 كإطار للتعاون الدولي بهدف تعزيز الأمن ألمعلوماتي وتحسين الثقة والأمن في مجتمع المعلومات، فضلا عن ذلك فان مجموعة دراسة (17) التابعة للاتحاد الدولي للاتصالات السلكية واللاسلكية تعمل بشكل فاعل من اجل تعزيز مبادرات الأمن الالكتروني وبضمنها كيفية تطبيق اقتفاء الأثر وآليات الجريمة الرقمية.

إن الاتحاد الدولي للاتصالات السلكية واللاسلكية هو ليس منصة دولية مثالية من اجل التعامل مع هذه القضايا الحساسة بسبب العضوية الكبيرة فضلاً عن قاعدة الإجماع في صنع واتخاذ القرار، ومع ذلك فانه من خلال مجموعات العمل الصغيرة يمكن إن تكون وسيلة لبناء مناقشات ثنائية موثقة.

توصية:

يجب إن تؤيد الولايات المتحدة الأمريكية وروسيا الاتحادية في إطار الاتحاد الدولي للاتصالات السلكية واللاسلكية فكرة عقد اتفاقية متعددة الأطراف وملزمة حول البنية التحتية الأساسية العامة. ويمكن أن يرتكز ذلك على تقييم السياسة المشتركة من قبل الخبراء الروسي والأمريكيين التي يمكن أن تعمل على تشخيص المشكلة وجعلها أكثر وضوحاً وإعطاء الحلول الممكنة من خلال تبنيها في اتفاقية ثنائية.

إن عقد اتفاقية ثنائية ملزمة حول البنية التحتية الأساسية سوف يساعد على تخفيض (المشكلة العشوائية) والمتأصلة للبنية التحتية المهمة في كلا البلدين. كما أن تبادل المعلومات بسهولة تحت رعاية الاتحاد الدولي للاتصالات السلكية واللاسلكية في المناقشات الذي سوف يمهد الطريق لمزيد من التعاون الدولي وهو الذي يخلف حافزاً لمزيد من التعاون بين الولايات المتحدة وروسيا الاتحادية حول عدد من القضايا السياسية الأخرى مثل مشروع الدرع الصاروخي وأفغانستان ومكافحة الإرهاب الدولي.

يجب أن يبدأ الإطار الأمريكي الروسي المشترك من خلال تحديد المطالب والرغبة في تبادل المعلومات، ويجب أن يعقب ذلك تقييم للمخاطر المشتركة لقطاعات معينـة مـع الإشـارة إلى أن التعاون الوثيق سوف يعود بالنفع على الجانبين. ومن ثم يؤدي ذلك إلى الترابط في حفـظ البنيـة التحتية الوطنية المهمة في البلدين كما أن تقييم المخاطر سوف يسهم في تحديد الإجراءات التـي يمكن اتخاذها مثل الحاجة إلى التشفير والتوثيق في قطاعات محددة.

إن هناك خشية متجـذرة بـين الأمـين العـام وحـق الخـصوصية الشخـصية في مثـل هـذه المناقشات. وقد أكد تقرير حول روسيا الاتحادية في عام 2002 على ما يأتي:

"الخصوصية هي مفهوم جديد يرتبط ارتباطا بالعملية التشريعية الروسية على الرغم من أن المشروع الروسي يحاول أن يعالج مسألة حماية البيانات الشخصية في المجـال الالكـتروني، كـما أن التوازن بين حقوق الأفراد والمرجعيـات الحكوميـة المختلفـة تميـل لـصالح الأخـير، لـذلك فـان أجهزة الأمن الروسية حصلت ومن خـلال تنـوع التـدابير التـشريعية عـلى حـق المراقبـة لجميـع أشكال المراسلات الالكترونية" .

الشيء المقابل للخصوصية هـو الأمـن، ومـن ثـم فـان المناقـشات حـول هـذه سوف يستمر على المستوى المحلي في الولايات المتحـدة بـشكل كبـير، وربمـا يتـسبب بردة فعل سياسية من جانب النشطاء السياسيين ومجموعات حقوق الإنـسان. يـرى مركز الدراسـات الإسـتراتيجية والدوليـة بأنـه " يجـب تبنـي أنظمـة التوثيـق بـشكل

واسع النطاق، كما أن المخاوف المتعلقة بالخصوصية يجب أن يتم معالجتها، ويمكن للمبادرة الجديدة أن تقوم بذلك من خلال جعل متطلبات المصادقة تتناسب مع المخاطر العالية ذلك أن الحالات الخطرة تتطلب تصديقاً عالي الدقة بينما حالات الخطر المنخفضة لا تتطلب منح التراخيص، والهدف هو تجنب وضع منهج واحد يتناسب مع جميع المناهج في عملية منح الاعتماد ومن ثم فان اي حوار بين الولايات المتحدة وروسيا الاتحادية يجب أن يأخذ هذا الأمر في الحسبان.

وفي النهاية، فان روسيا الاتحادية مشتركة في ترتيب "واسنر" الذي يحد من تصدير الأجهزة الصلبة والمرنة المتعلقة بالتشفير وعلى هذا الأساس فان أي تعاون فني يجب أن يتغلب على العقبة القانونية.

المحور السادس: مجموعة الثماني والتعاون في مجال الجريمة الالكترونية

تنشا معظم التهديدات (يوماً بعد يوم) حول تكامل البنية التحتية المعلوماتية عادة من النشاط الإجرامي الالكتروني بدلاً من الهجمات العسكرية التي تشرع بها الدول ضد بعضها البعض الآخر. كما أن المشكلة الرئيسة التي تواجه التعاون في مجال الجريمة الالكترونية هو الطبيعة المنتقلة للجرائم في الوقت الذي يجب على هيئات تنفيذ القانون أن تحترم الحدود.

إن التعاون بين الولايات المتحدة وروسيا الاتحادية حول الجريمة الالكترونية لم يسر بشكل منتظم في أفضل الأحوال في الماضي. وقد نشرت مؤخراً كثير من الدراسات حول الجريمة الالكترونية (الذي سبقه تعاون وثيق بين جهاز الأمن الفدرالي الأمريكي وجهاز الأمن الاتحادي الروسي)، وقد أشارت إليها بوصفها انطلاقة جديدة للتعاون بين البلدين، ومع ذلك فان إمكانات هذا التعاون لا تزال تحت الاختبار. وطبقاً للمتخصصين الروس. ليس هناك سبب حقيقي في أن لا يكون هناك تحقيق مشترك بين الولايات المتحدة وروسيا الاتحادية حول الجرائم الالكترونية، فضلا عن ذلك، يدور حول منظمة الانتربول خلاف كبير في روسيا الاتحادية ومن ثم فان التعاون معها سوف يكون صعباً للغاية، ولذلك لابد أن تكون هناك حاجة إلى قنوات دولية أخرى.

إن أهم محاولة بارزة ومتعددة الأطراف حول الجريمة الالكترونية هي " اتفاقية المجلس الأوربي بشأن الجريمة الالكترونية " التي دخلت حيز التنفيذ في تموز من العام 2004. وبحلول كانون الثاني من العام 2010 فان ثلاثة وعشرين دولة

من الدول الأعضاء في المجلس الأوربي صادقت على الاتفاقية، وخمس من الدول الأعضاء لم توقع عليها حتى الآن، إن هذه الدول الخمس وبضمنها روسيا الاتحادية التي تتحفظ على سيادتها وترى أن هذه الاتفاقية سوف تهددها. كما أن تركيا لم توقع على هذه الاتفاقية علاوة على أن ست عشرة دولة وقعت على الاتفاقية ولكنها لم تصادق عليها ومن أهم هذه الدول المملكة المتحدة والسويد وجورجيا وبلجيكا، كما يرى المتخصصون الروس " إن روسيا الاتحادية تستعد للتوقيع على الاتفاقية الأوربية المتعلقة بالجريمة الالكترونية " إذا ما رفع البند المتعلق بالسيادة، وقد وجه بوتين بالتصديق على الاتفاقية قبل سنتين ولكن وزارة الشؤون الخارجية الروسية أعاقته بسبب متطلبات المصلحة.

لقد وصف المجلس الأوربي الاتفاقية (بأنها الاتفاقية الدولية الملزمة الأولى حول الموضوع) التي تم تفعيلها حتى الآن وهي فريدة من نوعها في جوانب عدة:

أولا: تعالج الاتفاقية الممارسات والنشاطات غير القانونية التي تنشأ نتيجة مجموعة واسعة من تهديدات الأمن الالكترونية.

ثانيا: أنها المحاولة الأولى لتأسيس معايير وإجراءات مشتركة في مجال الأمن الالكتروني وفي الوقت ذاته تلزم موقعيها قانوناً.

ثالثاً: ن الاتفاقية مفتوحة للدول الأعضاء في المجلس الأوربي وغيرها من الدول، وهو الذي يعني بأنه من الممكن أن تكون أداة دولية مقبولة من قبل مجموعات أخرى من الدول (على سبيل المثال لقد وقعت الولايات المتحدة وصادقت عليها). وأخيرا وبشكل مثير للجدل، فان الاتفاقية تفي بمتطلبات

التعامل مع البيانات والوصول إليها التي تكون نتيجة المخاوف الناشئة عن حقوق الخصوصية والحقوق المدنية، كما هو الحال مع روسيا الاتحادية المتحفظة على مسألة سيادة الدولة.

وفضلا عن عمل المجلس الأوربي حول الأنظمة القانونية في هذا المجال فقد قدمت منظمة الأمن والتعاون الأوربي ومنظمة التعاون الاقتصادي والتنمية والأمم المتحدة العديد من المبادرات الالكترونية المتعددة الأطراف. ولكن طبقاً لتعزيز قسم الجريمة الاقتصادية في المجلس الأوربي ليس من هؤلاء المتمثلين من يمثل أساسا للتطبيق الفاعل أو التعاون الدولي، لان روسيا الاتحادية ليست عضواً في منظمة التعاون الاقتصادي والتنمية كما أنها رفضت الانضمام إلى اتفاقية الأمن الالكتروني. إن الأداة الرئيسة للتعاون بين الولايات المتحدة وروسيا الاتحادية هي المجموعة الفرعية (لمجموعة الثماني) حول جرائم التكنولوجيا المتطورة، كما ترأس كل منها الرئاسة الدورية لمجموعة الثماني.

لقد تشكلت المجموعة الفرعية لجرائم التكنولوجيا المتطورة كمجموعة فرعية عام 1996 بهدف مكافحة الجريمة المتنقلة والمنتظمة التي أوجدت شبكة من الاتصالات لجرائم التكنولوجيا المتطورة، وعمل 24/7، علاوة على دليل حماية البنية التحتية المعلوماتية الدولية الحساسة. كما عملت على طبع الوثائق والدليل العلمي للحاسوب وتقييم تهديدات الأمن الالكتروني انسجاما مع تنظيم مؤتمرات التدريب الدولي حول هيئات الجريمة الالكترونية، لقد شارك ممثلون من روسيا الاتحادية والولايات المتحدة في هذه المؤتمرات، كما أنهم

ساهموا في أعداد بعض الوثائق العملية القابلة للتطبيق. إن الدولتين ممثلتان في وفد المجموعة الفرعية المتخصصة التي تضم محققين في مجال الجرائم الالكترونية والمدعين العامين والخبراء من الأنظمة القانونية والطب الشرعي واتفاقيات التعاون الدولي.

تعد شبكة الاتصالات جرائم التكنولوجيا المتطورة الأولى من نوعها وقد انضمت أليها أكثر من عشرين دولة. لذلك تستمر الاتصالات في هذه البلدان على مدار الأربع وعشرين ساعة بهدف استقبال المعلومات أو طلبات التعاون المشترك والمتعلق بالجريمة الالكترونية. إن نقطة الاتصال المرتبطة بشبكة اتصالات مجموعة الثماني في الولايات المتحدة هي قسم الملكية الفكرية وجرائم الحاسوب في وزارة العدل الأمريكية وهي المسؤولة بدورها عن تنظيم أقسام الاستراتيجيات الوطنية المتعلقة بمكافحة انتشار جرائم الملكية الفكرية والحاسوب، أما في روسيا الاتحادية فجهة الاتصال هي جهاز الأمن القومي الفدرالي.

التوصية:

يجب أن توسع روسيا الاتحادية والولايات المتحدة شبكة البنية التحتية الموجودة في مجال الاتصالات المتعلقة بجرائم التكنولوجيا المتطورة تحت مظلة مجموعة الثماني بما في ذلك توفير إطار عالمي للاتصالات ودعم البرنامج العالمي لبناء القدرات في مجال تنفيذ القانون والتحقيق الالكتروني تجاه كل الدول

المرتبطة بشبكة المعلومات الدولية. لذلك فان هذه الآليات يجب ان تركز على ما يأتي:

1- تعزيز الشراكة الفاعلة بين صناع القرار والقطاعين العام والخاص، من اجل تبادل وتحليل المعلومات عن البنية التحتية الحساسة من اجل منع والتحقيق والاستجابة للمؤثرات والهجمات على البنية التحتية.

2- تأسيس شبكة طوارئ للإنذار المبكر لإصدار التنبيهات حول نقاط الضعف الالكتروني والحوادث.

3- الاشتراك في التعاون الدولي وتأمين البنية التحتية المعلوماتية الحساسة، لاسيما في مجال تنسيق التحقيقات حول الهجمات على بعض البنى التحتية بالانسجام مع القوانين المحلية.

إن الشبكة الدولية للاستجابة الطارئة سوف تعالج بشكل غير مباشر مشكلة الصراع الالكتروني من خلال التحديد السريع للتهديدات ومصادرها ومن ثم تمكين الحلول السريعة للقضايا القانونية مثل الولاية القانونية لقانون الجريمة الالكترونية.

فضلا عن ذلك، سوف يعمل تخفيض الجرائم الالكترونية عن طريق زيادة شبكات التعاون والبنية التحتية الحساسة على تعزيز الأمن. وكما ذكر المحللون الأمريكيون " يحتاج الأمن الفضائي الالكتروني أن يأخذ بنظر الاعتبار الانتظام. إن الجريمة الالكترونية تجعل شبكة المعلومات الدولية مكاناً فوضوياً في الوقت

الحاضر، ولو أننا تمكنا من إزالة الجريمة من الفضاء الالكتروني سوف يكون من السهولة بمكان للحكومات مواجهة الهجمات العشوائية على مواردهم الحقيقية، لذلك فأن تأسيس هذه الشبكة الدولية بالموازاة مع شبكات جديدة وآليات جديدة بضمنها عمليات التصديق سوف تكون خطوة أساسية في معالجة المشاكل العشوائية ومن ثم ردع الهجمات الالكترونية والجريمة الالكترونية".

يعد تأسيس الشبكة العالمية لنقاط الاتصال الخطوة الأولى في مجال التعاون الأمريكي الروسي بهدف مكافحة الجرائم الالكترونية والإرهاب الالكتروني. كما أن تحقيق الانسجام بين قوانين جميع البلدان والتعامل مع الحالات القانونية للمشاكل العشوائية سوف يكون ذا اثر بالغ. كما أشار جغيري كار (Jeffery Carr) في كتابه الموسوم (جوهر الحرب الالكترونية) بأن (الدول واقعة في مأزق بسبب فقدان المعايير المنهجية التي تجعل التعامل مع العشوائية أسهل بسبب أن الجهود المشتركة للتعرف على المهاجمين تستغرق وقتاً طويلاً كما أنها معقدة. كما أطلق عليها اسم (الاستجابة للازمات) أكثر من أي شيء آخر، لذلك فان الإسهام يتطلب الاستجابة الدائمة للازمة.

ومن دون إطار قانوني واضح، لن تأتي المساعدة من قبل الدولة المنشئة للاتفاقية بسهولة ويسر، حتى لو أصبح التعاون التقني في تعقب الهجمات فاعلاً بشكل كبير من خلال تأسيس الشبكة العالمية للاتصالات 24/7. وعلى هذا الأساس، فان هذا سوف يتبعه مبادرات قانونية واسعة النطاق.

المحور السابع: قانون الحرب الالكترونية ومنظمة الأمن والتعاون الأوربية.

تبقى الحرب الالكترونية ذات إطار قانوني واستراتيجي رمادي. وقد أسفرت المناقشات السياسية مؤخراً حول الموضوع إلى نتائج ضئيلة فيما يتعلق باتفاقية دولية ملموسة. وان فقدان القدرة على تحقيق تقدم ملموس متعلق بالمناقشات الجارية حول الحرب الالكترونية يعد أمرا مزعجاً إذا ما أخذنا بنظر الاعتبار الهجمات الالكترونية الأخيرة التي يُعتقد بأنها تمت برعاية دولة ما. كما تؤسس الاتفاقية المتعلقة بالحرب الالكترونية بروتوكولات حول ما هو السلوك المقبول وغير مقبول في الفضاء الالكتروني.

إن الأحكام يمكن أن تستثني البنية التحتية المدنية من أي هجوم الالكتروني في أي صراع مستقبلي بين الدول مع التأكيد على أن أي تجاهل للأحكام سوف يؤدي إلى تسويغ العقاب. لقد أكد العديد من خبراء القانون بان تحديثاً كبيراً للقوانين التي تحكم الصراع المسلح أصبح ذات ضرورة ملحة. وبشكل خاص فان تبرير استخدام القوة ضد الدول (فيما يتعلق بالحرب العادلة) يحتاج إلى إعادة تعريف واضح.

لقد كشف تقرير صادر عن المجلس الوطني للبحوث حول الآثار التكنولوجية والقانونية والأخلاقية والسياسية عن الاستخدام المحتمل واستخدام الهجوم والهجوم الالكتروني على قدرات الدول كما يأتي:

سوف يكون هناك شكوك حول كيف يمكن لقوانين النزاع المسلح وميثاق الأمم المتحدة أن يطبق في حالات كهذه. لذلك لابد من اتفاقية جديدة تعالج

هذه القضية كما أنها تحدد بوضوح ما هو المسموح به وما هـو غـير المـسموح بـه. لقـد أثبتـت التجارب التاريخية بان وجود قوانين واضحة في مجال الحرب هي دائما أفضل مـن وجـود أحكـام غامضة أو عدم وجود قوانين على الإطلاق.

أن وجود معاهدة حول الحرب الالكترونية هي مسألة حساسة في الساحة الدوليـة. ذلـك أن معظم وكالات المخابرات تستخدم التكنولوجيا الالكترونية بهدف اختراق البنية التحتية للدول الأخرى، وهذا يعد جزءاً من عملية جمع المعلومات لمدة عقود من الآن. في الواقع، الطـرق التـي تستخدم من قبل جواسيس الإجرام الالكتروني أو الإرهاب الالكتروني لا تختلـف اختلافـاً جوهريـاً عن بعضها الآخر. وعلى هذا الأساس، فان معاهدة تحظر على وجـه التحديـد هـذه الأنـواع مـن الأنشطة سوف تحظى بالدعم القليل مـن أي قـوة عالميـة كـبرى وسـوف يكـون مـن المـستحيل تنفيذها.

كما أن هناك تحدياً آخر يتمثل في انه سوف تواجه الولايـات المتحـدة الأمريكيـة وروسـيا الاتحادية أثناء محاولتهما تبني بروتوكول فاعل حول الأمن الالكتروني وتيرة بطيئة من المفاوضات المتعددة الأطراف تحت رعاية المنظمة الدولية. وفي الوقت الـسابق فـان المعاهـدة تـم إعـدادها وتطبيقها، وقد حظيت التكنولوجيا بأقسام كبيرة من المعاهدة والاهم من ذلك، هو أن المعاهدة التي تم التفاوض عليها بين الدول لا تشمل الفاعلين من غير الدول.

إن واحدة من أهم المعضلات التي تعترض محاولة المـضي قـدماً في تنظـيم الحرب الالكترونية في إطار القانون الـدولي هـي اختيـار المنتـدى الـدولي الفاعـل

والاهم لتحقيق ذلك. هناك العديد من الخيارات في هذا الشأن: اللجنة القانونية الدولية، مجلس الأمن الدولي التابع للأمم المتحدة، والجمعية العامة أو الاتحاد الدولي للاتصالات السلكية واللاسلكية، وإذا ما استثنينا أجهزتها الخاصة، ستؤدي هذه المنتديات حتماً إلى عملية طويلة الأمد لاسيما في العقود الأخيرة. ولهذا فانه من المنطقي تبني إستراتيجية للمواجهة وبنفس وتيرة اختيار المنتدى.

لقد قدمت روسيا الاتحادية لأول مرة فكرة معاهدة حول الحرب المعلوماتية. في عام 1998 على شكل مشروع قرار إلى الجمعية العامة للأمم المتحدة وترتكز فكرتها الأساسية حول فرض حظر على الأسلحة المعلوماتية. وخلال الدورة الرابعة والخمسين للجمعية العامة للأمم المتحدة قدمت روسيا الاتحادية مشروع قرار جديد وقد تم ذكر الإمكانات العسكرية للتكنولوجيا الالكترونية لأول مرة. وفي عام 2000، قدمت روسيا الاتحادية مسودة وثيقة مبادئ أخرى إلى الأمانة العامة للأمم المتحدة تتعلق بالأمن ألمعلوماتي الدولي.

لقد اعترضت الولايات المتحدة على عقد المعاهدة لأنها ترى من السابق لآونة مناقشة وإجراء مفاوضات حول اتفاقية دولية تتعلق بالحرب المعلوماتية. كما أن الولايات المتحدة حثت بدلاً من ذلك على تركيز الجهود حول تعاون دولي لمكافحة الجريمة الالكترونية والإرهاب الالكتروني، وان موقفها لم يتغير إلا بشكل ضئيل جداً. وإذا ما تم استثناء المؤثرات العسكرية لتكنولوجيا المعلومات فان الولايات المتحدة ترى بأن وجود ميثاق دولي هو أمر غير ضروري. وكما ذكرت الوثيقة الأمريكية للقمة العالمية للجمعية المعلوماتية فان قانون الصراع

المسلح ومبادئه الضرورية مناسبة وتحد من الأضرار الجانبية والتي تحكم أصلاً بعض الاستخدامات التكنولوجية.

التوصية:

يجب على الولايات المتحدة وروسيا الاتحادية إن تشرعا في إجراء تقييم مشترك للجوانب القانونية التي تنظم الحرب الالكترونية وبضمنها النشاطات الهجومية والدفاعية لاسيما في مجال البنية التحتية الحيوية وقواعد الاشتباك. كما أن التقييم يجب أن يقدم توصيات حول اختبار المنتدى الأكثر فعالية لتعزيز التحركات المتعددة الأطراف لتحقيق التنظيم.

أن تبني إستراتيجية للتغيير من الممكن أن تتضمن مجموعة من الدول القائدة، إذ من المحتمل أن تكون الولايات المتحدة وروسيا الاتحادية، أو بالإمكان أن تكون من خلال منظمة إقليمية تشترك فيها الدولتان.

تؤدي منظمة الأمن والتعاون الأوربية (OSCE) دوراً متزايداً في مجال تحديات الأمن الالكتروني، إذ أدت هذه المنظمة خلال السنتين الأخيرتين دوراً تعزيزياً متزايداً لاسيما بعد الحرب في جورجيا في آب 2008. وبعد مدة طويلة من تهميش منظمة الأمن والتعاون الأوربية فان أحداث جورجيا جعلت المنظمة تعود إلى دائرة الأضواء الدولية كما كانت خلال مدة الحرب الباردة. وعلى هذا الأساس يبدو من المفيد لروسيا الاتحادية والولايات المتحدة أن يسعيا إلى دعم أي مبادرة حول الحرب الالكترونية تتم من خلال قنوات منظمة الأمن والتعاون

الأوربية والاستفادة من تعاظم دور المنظمة في الآونة الأخيرة. كما أن روسيا الاتحادية لا تزال متشككة ولديها نظرة عدائية تجاه هذه المنظمة.

لقد كان دور منظمة الأمن والتعاون الأوربية قبل الهجمات الالكترونية على استونيا علم 2007 والحرب على جورجيا ضئيلاً جداً. وفي كانون الأول من العام 2004، عمل المجلس الوزاري (الذي يتألف من وزراء خارجية دول منظمة الأمن والتعاون الأوربية والدول المشاركة) على معالجة التوسع في استخدام شبكة المعلومات الدولية من قبل المنظمات الإرهابية وتتضمن هذه النشاطات ما يأتي: تجنيد الإرهابيين وعمليات التحويل والتنظيم والدعاية.

وعندما تسنمت استونيا رئاسة منظمة الأمن والتعاون في العام 2008 اقترحت منهجا شاملا تتبناه المنظمة في مجال قضية الأمن الالكتروني. وعندما عقدت المنظمة ورشة عمل حول المنهج الشامل للمنظمة في مجال الأمن الالكتروني في عام 2009، كانت توصياتها تتضمن تفعيل التعاون الذي تم تبنيه من المجلس الوزاري. وقد شاركت الولايات المتحدة وروسيا الاتحادية في ورشة العمل.

يرى العديد من المتخصصين ضرورة عدم الاستعانة بمنظمة الأمن والتعاون الأوربية كأداة للنهوض بالقانون الدولي فيما يتعلق بالأمن الالكتروني. وبالطبع، من المرجح أن منظمة الأمن والتعاون الأوربية سوف لن تستطيع التوصل إلى اتفاق نهائي بسهولة ويسر حول معاهدة تتعلق بهذا المجال. ولكن إذا ما تمكنت منظمة الأمن والتعاون الأوربية من تهيئة فرصة مناسبة

للنقاش وإعادة تعريف القضايا كما تفعل الأمم المتحدة فمن الممكن أن تكون الخيـار الأفـضل. كما أن تبني المبادئ ضمن إطار منظمـة الأمـن والتعـاون الأوربيـة لـن يحـول دون التوصـل إلى اتفاق حول البرتوكولات المستقبلية التي يتم تبنيها في إطار الأمم المتحدة.

المحور الثامن: روسيا الاتحادية وحلف شمال الأطلسي

لقد غطت صحيفة " روسكي نيوزويك " الأسبوعية في نسختها التي تصدر باللغة الروسية في عددها الصادر في 23 تشرين الثاني غلافها بقصة أشارت فيها إلى القراصنة الروس الكبار الذين يعملون في الداخل والخارج. كما أنها استخدمت مصطلحات مثل " الإمبراطور الالكتروني الشرير " والحرب الباردة الالكترونية. وفي الوقت نفسه، يحاول حلف شمال الأطلسي أن يدرك كيف سيتم التعامل مع قضايا الأمن الالكتروني، وهل أن الهجمات الالكترونية على دولة عضو في منظمة حلف شمال الأطلسي يستدعي الالتزام المنصوص عليه في المادة (الخامسة) من اتفاقية الدفاع المشترك.

خلال الحرب الباردة، كان البعد الجيوسياسي يرتكز على الحدود وسبل الدفاع عنها، بينما تدور الدبلوماسية الالكترونية في القرن الحادي والعشرين حول ليس فقط إدارة عالم بلا حدود بل يمكن أن يدار بشكل أفضل عندما يكون الربط فاعلاً وبشكل سلس. إن هذا العالم الذي يعتمد بشكل كبير على استقرار التعاملات المالية والتبادل التجاري العالمي لا يمكن أن يعمل بشكل فاعل إذا ما تمكن القراصنة من مهاجمته بشكل كبير.

لذلك كيف يمكن لحلف شمال الأطلسي المؤطر بإطار جغرافي معين أن يحاول إعادة تعريف علاقته مع روسيا الاتحادية، فضلا عن ذلك كيف يمكن إدراك دوره في تعزيز الدبلوماسية الالكترونية والسلام الالكتروني؟، كيف سيكون الهيكل المؤسسي والاستراتيجي لحلف شمال الأطلسي إذا ما تعرضت

إلى التهديدات الأمنية الكبيرة في العشر سنوات القادمة من قبل الإرهابيين أو الدول مع تقدم القدرات الهجومية؟.

إن التغيير الأكبر سوف يكون في مجال التجسس، كما انه سوف يستمر إذا ما تغيرت العناصر الأساسية. كما ستعمل روسيا على تغيير أولويات تجميع المعلومات في دول حلف شمال الأطلسي، وستعمل الولايات المتحدة على تغيير أولوياتها التجسسية في روسيا الاتحادية. وعلى هذا الأساس، فان كل الأطراف سوف تعمل على الأقل على حماية أسرار الآخرين بدلاً من سرقتها لان ذلك يدعم الأمن الاقتصادي لهما.

وفيما يتعلق بحلف شمال الأطلسي، فان الوقت قد حان لجعل الأمن الالكتروني في قمة أولويات القضايا الرسمية في تعامله مع روسيا الاتحادية. كما إن الجانبين لهما مصالح مشتركة في البحث عن حلول مشتركة وليس فقط نظرة كل منهما للآخر بوصفه التهديد الأكبر.

وفي خطاب لنائب رئيس الولايات المتحدة بالاشتراك مع رئيس هيئة الأركان المشترك الجنرال جيمس كارترايت في حزيران من العام 2009، أعطى لمحة عن ظهور المفهوم الاستراتيجي للقوة العسكرية العالمية الوحيدة التي أطلق عليها " الضربة العالمية " وقال بان الهدف الأدنى النهائي لهذه الضربة العالمية هو أن تكون في أي مكان على سطح الأرض في غضون ساعة، بينما الهدف الأعلى هو أن تكون في أي مكان على سطح الأرض في غضون ثلاثمئة ميل بالثانية وهذا هو الالكتروني، وقد تم الإفصاح عن ذلك من خلال مناقشة الرؤية لأربع

سنوات قادمة فيما يتعلق بالتخطيط والقدرات العسكرية للدولـة، وقـد تبعتهـا رؤيـة كاتريـات وتساءلت كيف سيكون شكل الردع في القرن الحادي والعشرين.

وبالإشارة إلى انتشار الصواريخ البالستية العابرة للقـارات، لاحـظ كارتريـات بـان هجومـاً جديداً [من المحتمل أن يكون نووياً] من الممكن أن يكون في غضون ثـواني قليلـة. كـما قـال: أن هذه الأوضاع تتطلب شيئاً من الردع أكـثر مـن الـردع النـووي. وحـسب جهـة نظـر وفي معـرض حديثه قال: تقع قواعدنا العسكرية في الأماكن التي قابلنا فيها الهنود واليابـانيين والألمـان، لـذلك اعتقد بان حقائق القواعد الحالية لا تفي بمتطلبات الردع أو الاستجابة للتهديدات الجديدة.

المحور التاسع: الحضور الالكتروني الأمريكي في أوروبا

لقد استجابت الولايات المتحدة للتهديدات الأمنية الناشئة من خلال تحريك قواتها وقواعدها في أوربا الصغيرة كما هي من خلال تحويلها إلى الشرق أو الجنوب بهدف جعلها ترتبط ببؤر التوتر في الشرق الأوسط أو القرن الأفريقي. وفي عام 2004 بدأت الولايات المتحدة الأمريكية تخطط لإغلاق ما يقرب من نصف قواعدها العسكرية (589) في أوربا نتيجة لمراجعة الوضع العالمي. وعلى هذا الأساس فان الولايات المتحدة الأمريكية هي الآن الأكثر اهتماماً في " المواقع الأمنية التعاونية " من القواعد العسكرية التقليدية وقد خصت الولايات المتحدة دول البحر الأسود مثل رومانيا وبلغاريا بوصفها أهدافا أساسية لإعادة التوجه الجديد لحضور الولايات المتحدة وتأسيس المواقع الأمنية التعاونية.

لقد تأكد ذلك من خلال المعالجة الحالية لتهديدات الصواريخ الباليستية العابرة للقارات والصواريخ النووية في دول الشرق الأوسط. لذلك فان الولايات المتحدة وحلف شمال الأطلسي يوليان اهتماماً متزايداً بمنطقة البحر الأسود. وهذا يعني بان القدرات الحربية الالكترونية جنباً إلى جنب مع عملية جمع المعلومات المرتبطة بها ومتطلبات العمليات السرية من المرجح أن يتم بناؤها هناك. وهذا التركيب الجديد من المحتمل أن يدفع الولايات المتحدة إلى إعادة تشكيل علاقتها مع دول البحر الأسود: روسيا، أوكرانيا وجورجيا (وبضمنها ابخازيا) ورومانيا وبلغاريا وتركيا.

المحور العاشر: المناورات والتبادل العسكري الالكتروني

شهدت العلاقات الروسية مع حلف شمال الأطلسي نكسة حادة في أعقاب الحرب الروسية ضد جورجيا في آب من العام 2008. بل أن بعض المحللين وضع مقارنات لزمن الحرب الباردة. فقد شهدت العلاقات فتوراً قبل فترة قليلة من الحرب لاسيما عندما تقدمت جورجيا وأوكرانيا بطلب العضوية إلى حلف شمال الأطلسي. إذ أكد رئيس الوزراء الروسي السابق(الرئيس الحالي) فلاديمير بوتين بان انضمام أوكرانيا إلى حلف شمال الأطلسي ربما يعرض وجودها كدولة ذات سيادة إلى خطر. كما أن هناك احتمالاً كبيراً في تورط الحكومة الروسية في الهجمات الالكترونية على البنية التحتية الحيوية الجورجية خلال الصراع الجورجي الروسي، وقد بقى ذلك موضع شك ونقاش.

لقد ذكر مشروع كري كوس وهي منظمة غير حكومية مقرها الرئيس الولايات المتحدة في تشرين الثاني من العام 2008 بان الهدف الأساسي هو: نحن نعتقد بثقة عالية بان الحكومة الروسية من المحتمل أن تستمر في سلوك النأي بنفسها عن القراصنة الوطنيين الروس الذي يتمتعون بالإنكار الخفي ولذلك فهي تدعم بالخفاء وتتمتع بالمنافع الإستراتيجية الناجمة عن نشاطاتهم إلا أن الحكومة الروسية أنكرت مراراً وتكراراً وبشدة أي تورط لها بهذا الشأن. أن العلاقات الروسية مع حلف شمال الأطلسي تتحسن ببطء على الرغم من أن الشكوك تبقى قائمة لاسيما في مجال الأمن الالكتروني. وفي هذه الأثناء يناقش حلف شمال الأطلسي ويعمل على إعداد مفهوم الإستراتيجية الجديدة له

استناداً إلى مسألتين هما مستقبل العلاقة الروسية مع حلف شمال الأطلسي ودور الأمن الإلكتروني في مجال التخطيط الأمني المستقبلي لحلف شمال الأطلسي.

يعد مجلس (روسيا – حلف شمال الأطلسي) الهيئة الأساسية للترابط الرسمي بين حلف شمال الأطلسي وروسيا الاتحادية. لقد تأسس هذا المجلس عام 2002 في أعقاب هجمات الحادي عشر من سبتمبر الذي كان يهدف إلى التأكيد على الحاجة للعمل التنسيقي لمواجهة التهديدات المشتركة مثل الإرهاب. يؤدي المجلس وظائف عديدة من خلال سبعة وعشرين لجنة ومجموعات العمل المسؤولة عن مجالات سياسية مختلفة. وان احد مجموعات العمل هو منتدى التعاون العلمي الروسي مع حلف شمال الأطلسي الذي يعد من بين أدوات أخرى وسيلة من وسائل التعاون في مجال الأمن الإلكتروني.

لقد شكل حلف شمال الأطلسي " مركز التميز (Center of Excellence) " للدفاع الإلكتروني في استونيا لدراسة وتحديد الهجمات الالكترونية وتحت أي ظرف من الظروف، وفي مثل هذا الأمر، لابد من أن تؤدي هذه الهجمات إلى تفعيل مبادئ الدفاع المشترك لحلف شمال الأطلسي الذي ينص على (إن هجوماً على احد الأطراف يجب أن يعد هجوماً على الكل). كما أن مهمتها الأخرى تتمثل في تحسين القدرات والتعاون وتبادل المعلومات بين دول حلف شمال الأطلسي ومن خلال الدروس الماضية المستفادة. لقد تم تأسيس المركز في عام 2008 كما أن العضوية مفتوحة إلى كل دول حلف شمال الأطلسي.

التوصية:

على المستوى السياسي يجب على روسيا الاتحادية وحلف شمال الأطلسي أن يلتزما بإكمال التقييم المشترك في غضون مدة زمنية معينة (على سبيل المثال سنتين) حول ما الذي يشكل الأمن الالكتروني العالمي وكيف يمكن تحقيقه. وفي إطار التعاون العلمي الروسي مع حلف شمال الأطلسي يجب أن يشتركا في المراقبة المتبادلة والمشاركة في التعامل مع الهجمات الالكترونية. وفي إطار الشراكة مع حلف شمال الأطلسي يجب أن يطور البلدان منهجيات ومعايير لتقييم مدى التأثير والاشتراك في المرافق الحيوية.

فضلا عن ذلك، فان عدم الأخذ بهذه التوصية يجب أن لا يستبعد المشاركة في المناورات العسكرية الالكترونية مهما كان المناخ السياسي الحالي، وعندما قامت الولايات المتحدة بعملياتها العسكرية، عملت القوات المسلحة الروسية على تطوير عقيدة عسكرية الكترونية عتيدة صممت للعمل كقوة متعددة الأبعاد.

كما أشار التقرير الذي صدر مؤخراً بأنها تتضمن القدرة على تعطيل البنية التحتية للمعلومات العائدة إلى أعداء روسيا الاتحادية وتعطيل الأسواق المالية وقدرات الاتصالات العسكرية والمدنية. إن حساسية وسرية هذه القدرات تحول دون تحقيق أي شكل من أشكال التعاون. وهناك سبب واحد هو نشاطات واليات مخابرات البلدين في مجال التجسس الالكتروني وعلى الرغم من أن الحرب الباردة انتهت قبل عشرين عاماً إلا أن الشكوك المتبادلة من الصعب

التغلب عليها. ولكن يتفق الخبراء بان الطرق المستخدمة من قبل المحاربين الالكترونيين لا تختلف عن تلك المستخدمة من قبل المجرمين الالكترونيين والإرهاب في المجال الالكتروني وبذلك يتفق الطرفان على التهديدات الأساسية للبنية التحتية لهما. إن زيادة تبادل المعلومات المشتركة خلال المناورات المشتركة سوف يزيد من قدرة البلدين على حماية نفسها في تهديدات كهذه. ومن وجهة النظر الفنية من المهم ملاحظة ليس هناك تكامل للقوة في مجال الأمن الالكتروني إذ أن بإمكان أي شخص الدخول إلى المسارات التي ينتجها النظام نفسه، وهكذا من قبيل المبالغة إذا قلنا بان المنظمات والوزارات والدول هي فقط تكون معرضة للهجوم الالكتروني لدرجة أنهم يسمحون لأنفسهم أن يكونوا كذلك، وعلى هذا الأساس فان التعاون في هذا المجال له منافع مشتركة.

أن الحوار مع القطاع الخاص لاسيما مع الصناعات العسكرية يمكن أن يبدأ تحت مظلة مجلس (روسيا – حلف شمال الأطلسي). كما أن المتخصصين في كل بلد لديهم صعوبة حول كيفية عمل القطاع الخاص والهيكل الحكومي في البلد الآخر لان دور الحكومة دور مركزي في كل جانب من جوانب الأمن الالكتروني وان كثيرا من عبء تنفيذ الاستراتيجيات الوقائية يقع على عاتق القطاع الخاص، فان تحسين التآلف مع المسؤوليات التنظيمية والخبرات العلمية سوف يعود بالنفع على العديد من المتخصصين في البلدين على الرغم من الاختلافات الهيكلية الواضحة في تشكيل القطاعات الدفاعية لروسيا الاتحادية والولايات المتحدة الأمريكية من حيث الملكية الحكومية.

تختلف رؤية حلف شمال الأطلسي عن الرؤية الروسية فيما يتعلق بأهمية مجلس (روسيا الاتحادية – حلف شمال الأطلسي) لاسيما في مجال إدارة العلاقات المتبادلة. وفيما يتعلق بروسيا الاتحادية يهدف المجلس دائماً إلى أن يكون منصة أساسية لمناقشة العلاقات الروسية مع حلف شمال الأطلسي، بينما لم تنظر الدول الأساسية في حلف شمال الأطلسي إلى المجلس على انه مجلس موضوعي، كما انه فشل في إزالة أو إصلاح الخلافات السياسية والتنظيمات بين حلف شمال الأطلسي وروسيا الاتحادية. ويرى بعض المحليين أن السبب الوحيد الذي جعل روسيا الاتحادية متمسكة بالمجلس هو المنفعة السياسية الخالصة المتمثلة في العمل على تهميش منظمة الأمن والتعاون الأوربية التي كان لها دور بارز في مراقبة الانتخابات الروسية ووضع ما بعد الصراع في جورجيا.

ونظراً للسرية التامة التي يحيطها كلا البلدان حول قدراتهما الالكترونية ليس من المستغرب أن يكون هناك تردد كبير للدخول في تعاون عسكري في هذا المجال. إن التبادل الأولي يمكن أن يكون مقتصراً على المعلومات غير مصنفة في إطار مجلس (روسيا – حلف شمال الأطلسي)، ومن ثم من الممكن أن يتبع ذلك تبادلان متعددة ملموسة أكثر حول سيناريوهات التهديد المتبادلة المحددة مثل حماية البنية التحتية الحيوية (مثل المفاعلات النووية) من الهجمات الالكترونية خلال أوقات الحرب، كما أن الشفافية فيما يتعلق بكل جوانب القدرات الحربية المعلوماتية غير مطلوبة، فضلاً عن انه ليس هناك حاجة لتبادل المعلومات السرية في العمليات الداخلية للحكوميين.

المحور الحادي عشر: الخطوط الأخرى للعمل

يجب أن تدعم الأمثلة الأربعة الملموسة للتعاون التي ذكرت سابقاً من خلال مبادرات ومشاريع أخرى مثل تقييم التهديدات المشتركة وتطوير المصطلحات المشتركة مثل (الأمن الالكتروني مقابل الأمن المعلوماتي).

إن معهد قضايا الأمن ألمعلوماتي التابع لجامعة موسكو (ليمونوسوف) عين رسمياً من مجلس امن روسيا الاتحادية بوصفه المنظمة العالمية الرائدة في روسيا الاتحادية للتعامل مع قضايا الأمن المعلوماتي والتعاون الدولي. كما أن الاتصال بين معهد قضايا الأمن ألمعلوماتي وجامعة الأمن القومي الأمريكية موجود أصلا ولكن يجب تكثيف هذه الاتصالات في مختلف المجالات لاسيما في موضوع حساس كالحرب الالكترونية. كما أن مشاريع البحث المشتركة قد تؤدي الى تحسين قدرات التعامل مع المشاكل العالمية المرتبطة بالجانب الالكتروني. فعلى سبيل المثال اقترح احد خبراء الأمن الالكتروني الأمريكي إنشاء شبكة تحذير الكتروني مبكر، وهذه الفكرة يمكن أن تشكل أساسا مشتركاً لخبراء الولايات المتحدة وروسيا الاتحادية في أحدى المنتديات الدولية مثل الاتحاد الدولي للاتصالات السلكية واللاسلكية وهو الأمر الذي سوف يساعد على توسيع الاتصالات والتعاون الدولي بين الجامعات الروسية والأمريكية ومراكز البحوث، كما أن القطاع الخاص سوف يعمل على تقديم المساعدة بهدف التغلب على انعدام الثقة.

لقد طلب الخبراء الروس تأسيس مركز عالمي لرصد وتحديد وتقييم التهديدات في المجال المعلوماتي وتأسيس آليات دولية للتشاور حول المشاكل المستعصية بهدف ضمان الأمن المعلوماتي الدولي. وقد حضي هذا الطرح باهتمام ضئيل على المستوى الدولي، كما أن المسؤولين الحكوميين الأمريكيين كانوا أكثر حذراً فيما يتعلق بالجانب الداخلي. ومع ذلك فان مجلس النواب الأمريكي عمل على تشريع قانون الأمن الالكتروني في آذار من العام2010 ، كما يرى رئيس لجنة العلم والتكنولوجيا في مجلس النواب بان تحسين الأمن الالكتروني يتطلب جهداً تعاونياً على المستوى الداخلي والدولي.

الخاتمة:

سيبقى فيما إذا كان التعاون الحقيقي والفعال ممكناً بين روسيا الاتحادية والولايات المتحدة حول الأمن الالكتروني. كما انه ليس هناك قصور في القادة السياسيين والخبراء الأمنيين في البلدين الذي يرون أن العلاقة تقوم على المواجهة بشكل أساسي: تهديدهم بالهجوم يقابله إجراءات دفاعية. أن فكرة الأمن المشترك في المجال الالكتروني لهؤلاء الأشخاص ليس فيها كثير من الإغراءات. مع ذلك فان نقاط الضعف المشتركة الهائلة: طبقاً للمعلومات الرسمية تتمثل في السجلات المصرفية والرقابة على الأجهزة الطبية الحساسة والسيطرة على محطات القوة النووية والصواريخ النووية الباليستية. وعلى هذا الأساس فان مفاهيم السياسة القديمة يجب أن تتغير. إنها مفاهيم عفا عنها الزمن مثل الردع من خلال التدمير المتبادل المؤكد، إذ أصبح لا معنى له في مجال الفضاء الالكتروني. إذا تمكنت الولايات المتحدة وروسيا الاتحادية من البدء بفتح مجالاتهما الالكترونية بشكل أكثر اتساعاً فان هذه خطوة أساسية تجاه بناء الثقة وتامين البنية التحتية المعلوماتية وتعزيز مسألة نشر المعلومات على المستوى العالمي.

References:

1- “President Obama’s Remarks on Securing U.S. Cyber Infrastructure,”May29, 2009 , http://www.america.gov/st/texttransenglish/2009/May/20090529161700eaifas0.1335871.html.

2- James A. Lewis et al., Securing Cyberspace for the 44th Presidency : A Report of the CSIS Commission on Cybersecurity for the44th Presidency, Washington, D.C., CSIS, December2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

3- Russian Federation, Information Security Doctrine of the Russian Federation, September, 2000,
http://www.mid.ru/ nsosndoc.nsf /1e5f0de28fe77fdcc32575d900298676 2deaa9ee 15ddd24bc32575d9002c442b?Ope Document.

4- Joint Statement on Common Security Challenges at the Threshold of theTwenty-First Century, September 2, 1998. See Weekly Compilation of Presidential Document (http://www.gpoaccess.gov/wcomp/) with text Available at:
http://frwebgate1.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=64826251485+510 WAISaction=retrieve.

5- Kristin Archick, “Cybercrime: The Council of Europe Convention , ”CRS Report, 2004 ,http://fpc.state.gov/documents/ organization/36076.pdf.

6- “Convention on Cybersecurity, ” Council of Europe, (CETS No.: 185http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=05/04/2010&CL=ENG.

7- Marina Volkova, "Cybercrime should be stamped out by entire world, " Voice Russia, March22, 2010: http:// english .ruvr.ru /2010/03 /22/5520499.html.

8- "Working Meetings: Summit 2006," G8 Summit 2006, Moscow, November28-30, http:// en.g8russia.ru /page_work /32.html. "G8 Initiative For Public-Private Partnerships To Counter Terrorism: Private Sector Action Beyond 2006, " (EastWest Institute, November 2006. The EastWest Institute supported the Russian government's initiative by convening preparatory meetings and helping to mobilizeprivate sector participation), http:// www.ewi.info/ public-private- partnerships-combat-terrorism.

9- Sergei Komov, Sergei Korotkov, and Igor Dylevski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law, " (Disarmament Forum, 2007, No. 3), http://www.unidir.ch/pdf/articles/pdf-art2645.pdf.

10- "Developments in the Field of Information and Tele communications in the Context of International Security, "United Nations General Assembly, A/Res/53/70, January12, 1999: http://daccess-dds-ny.un.org /doc/UNDOC /GEN /N99/760/03/ PDF / N9976.

11- "UN Information Department, Report on the Plenary of the 64th General Assembly, " GA/10907, December 21, 2009:

http:// www.un.org/News/Press/docs/2009/ga10907.doc.htm:"TheAssembly invited Member States to use the voluntary self-assessment tools, as listed in the draft's annex, toprotect critical information infrastructures and strengthen cybersecurity toaid national efforts and highlight areas for further action."

12- “On 3 September 2008, IMPACT and the ITU formally entered into a Memorandum of Understanding (MoU) in which IMPACT’s state-of-the-art Global HQ in Cyberjaya, Malaysia, effectively became the physical and operational home of the GCA. Under this landmark collaboration, IMPACT provides the ITU’s 191 Member States with the expertise, facilities and resources to effectively address the world’s most serious cyber threats.” http://www.impact- alliance.org /about_collaboration.html.

13- A similar resolution had been approved each year by the General Assembly since 1998 without a vote but with the explicit disapproval of the United States.

14- “Developments in the Field of Information and Telecommunications in the Context of International Security, ” United Nations General Assembly, A/RES/64/25, December 2, 2009.

15- Office of the Spokesman,“Roundtable on U.S.-Russia Information , Technology : Dialogue on a range of topics including broadband and

Internet governance, ” U.S. Department of State, May 10, 2010, http://www.america.gov/st/texttransenglish/2010/May/20100510144916xjsnommis0.4230245.html.

16- Myriam Dunn Cavelty, “Critical Information Infrastructure: Vulnerabilities, Threats and Responses, ” Disarmament Forum, no. 3, September 2007.

17- James A. Lewis et al., Securing Cyberspace for the 44th Presidency, p. 34.

18- Jan Softa, Threats Against Russia's Information Society (Charleston, S.C.:BookSurge, 2008), p. 22.

19- 19 Lewis et al., Securing Cyberspace for the 44th Presidency, p. 23.

20- Softa, Threats Against Russia's Information Society, p. 23.

21- Federal'naya sluzhba bezopasnosti.

22- Elgin Brunner and Manuel Suter, "Russia—Critical Sectors, " in An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, ed. Andreas Wenger, Victor Mauer, and Myriam Dunn (Zurich: Center for Security Studies, ETH Zurich, 2008), p. 347.

23- Ibid, p. 342.

24- A. A. Streltsov, Gosudarstvennaya informatsionnaya politika: osnovy teorii, State Information Policy: The Basis of the Theory, (Moscow, 2010), p. 77.

25- Ibid.

26- Ibid, p. 342. For example, in 2001 the "Electronic Russia" program was launched. Its main purpose is to increase the efficiency of the Russian economy, improve management in the public sector,and enhance self-government by applying information and communication technologies.

27- Ibid, p. 345.

28- John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cybersecurity, " New York Times, June 27, 2009, p. A1.

29- Brunner and Suter, “Russia—Critical Sectors, ” p. 346.

30- S. Shestakov, Representative of the Russian Federation, ”Joint meeting of the OSCE Forum for Security Co-operation and the OSCE Permanent Council, ” (June 12, 2010): http:// www.osce.org/documents / fsc/2010/06/44705_en.pdf.

31- White House Blog, “Introducing the New Cybersecurity Coordinator,”http:// www.whitehouse.gov /blog/2009 /12/22/ introducing-new-cybersecuritycoordinator (posted December 22, 2009).

32- Brunner and Suter, “Russia—Critical Sectors, ” pp. 635–37.

33- John Rollins and Anna C. Henning, “Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, ” Congressional Research Service Report for Congress, March 10, 2009, p3.

34- Brunner and Suter, “Russia—Critical Sectors, ” pp. 635–37.

35- “United States Views on Information Network and Infrastructure Security in the WSIS Action Plan, ” position paper presented at the South East European Cooperation Conference, (Sofia, Bulgaria, September 8–9, 2003).

36- White House, Executive Office of the President, Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure (May 29, 2009) :http:// www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

37- Ibid.

38- Ibid.

39- Lewis et al., Securing Cyberspace for the 44th Presidency, p. 23.

40- Rollins and Henning, “Comprehensive National Cybersecurity Initiative, ” p. 3.

41- Markoff and Kramer, “U.S. and Russia Differ on a Treaty for Cybersecurity.”

42- John Markoff and Andrew E. Kramer, “In Shift, U.S. Talks to Russia on Internet Security,” New York Times, December 12, 2009, p. A1.

43- Bruce Jones, “Moscow and Washington Seek Cyber Security Regulations, ”Jane’s Defence Weekly, January 6, 2010, p. 6.

44- Private meeting, April 24, 2009.

45- This list is a modified version of topics identified during preparatory meetings organized by EWI for Russia’s G8 initiative in 2006 on public-private partnerships to counter terrorism.

46- EWI Interview, ranz-Stefan Gady and Liza Kurukulasuriya, Moscow, March2010. One of the most challenging aspects in the field of cybersecurity is the problem of attribution, i.e., tracing back an action in the cyber sphere to its originator, be it an individual, an organization, or a state. Public Key Infrastructure is used for encryption of data, electronic signatures (i.e., nonrepudiation), and authentication of users.

47- Interview, Moscow, March 2010.

48- “National Strategy for Trusted Identities in Cyberspace, ” pp. 13–14, June 25, 2010,http:// www.dhs.gov/ xlibrary /assets/ns_tic.pdf.

49- Ibid, p.29. The document had a very short section on international cooperation:“The Federal Government will prioritize and appropriately staff existing international efforts associated with trusted digital identities. As discussed previously, standards development and adoption at the international level is a cornerstone of global commerce and information exchange. To avoid localized standards development and adoption, domestic efforts should endeavor to adopt international standards whenever they are consistent with domestic goals.”

50- According to searchsecurity.com: “A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message.”:http:// searchsecurity. techtarget.com/sDefinition/0, , sid14_gci214299, 00.htl.

51- Report on Background and Issues of Cryptography Policy, Directorate for Science, Technology and Industry, Organization for Economic Cooperation and Development, 1997, ttp://www.oecd.org/document/36/0, 3343, en_2649_34255_1814820_1_1_1_1, 00.html.

52- Global Cybersecurity Agenda: Framework For International Cooperation in Cybersecurity, nternational Telecommunication Union, 2007, p. 8.

53- Lewis et al., Securing Cyberspace for the 44th Presidency, p. 49.

54- Kelly Jackson Higgins, "Do Official Says U.S. Needs Separate Cyber czar For Online Identity, " DarkReading.com, July302009: http:// www.darkreading.com/ security/government /showArticle.jhtml?articleID=218900177.

55- Lewis et al., Securing Cyberspace for the 44th Presidency, p. 49.

56- Top Cyber Security Problems that Need Resolution—The Planetary Emergency Regarding the Insecurity of Global Communications, World Federation of Scientists, Permanent Monitoring Panel on Information Security, January 11, 2010.

57- Valerie Abend et al., "Cyber Security for the Banking and Private Sector, "in Wiley Handbook of Science and Technology for Homeland Security, ed.John G. Voeller (New York: Wiley, 2008); Elena G. Efimova and Maria K.Tsenzharig, "Electronic Logistics Services in Russia: The Bridge to United Europe, " Electronic Publications of Pan-European Institute, March 2009, http://www.tse.fi/FI/yksikot/erillislaitokset/pei/Documents/Julkaisut/Efimova%20and %20Tsenzharik%200309%20web.pdf.

58- Markoff and Kramer, "U.S. and Russia Differ on a Treaty for Cybersecurity."

59- "…The Strategy defines and promotes an Identity Ecosystem that supports trusted online environments. The Identity Ecosystem is an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities…. Privacy protection and voluntary participation are pillars of the Identity Ecosystem. The Identity Ecosystem protects anonymous parties by keeping their identity a secret and sharing only the information necessary to complete the transaction."National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy, Draft Paper,(Washington DC, June 25 2010,) http://www.nstic.ideascale.com/.

60- Russian Association of Networks and Services, http://www.rans.ru/eng/About /.

61- Ibid.

62- International Telecommunications Union, X.509: Information technology: Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, http://www.itu.int/rec/T-REC-X.509.

63- Stein Schjlberg, Report of the Chairman of High Level Experts Group (HLEG), TU Global Cybersecurity Agenda, September2008,http://www.itu.int/osg/csd/cybersecurity/gca/docs/ Report _of_ the_Chairman_ of_HLEG_to _ITU_SG_03_sept_ 08.pdf.

64- Dependability Development Support Initiative, RAND Europe, National Dependability Policy Environments: Russian Federation, November 2002, 11.http:// www.ddsi.org /htdocs/Documents/final%20docs/DDSI_Country_Reports_Final_Russia.pdf.

65- Lewis et al., Securing Cyberspace for the 44th Presidency, p. 64.

66- For further information on the cryptography agreement in the Wassenaar framework, see http:// www.international.gc.ca /controls controles /abouta_ propos/export /Wassenaar _crypto.aspx?lang=eng.

67- Joseph Menn, “Moscow cracks down on cybercrime, ” CNN, March 25, 2010, http:// www.cnn.com /2010/BUSINESS /03 /22/moscow.cybercrime.ft /index.html.

68- EWI Interview, Moscow, March 2010.

69- Council of Europe, Convention on Cybercrime, (Budapest 23.XI.2001)http://conventions.coe.int/treaty/en/treaties/html/185.htm.

70- “Putin Defies Convention On Cybercrime”, Computer Crime Research Center, March 28, 2008: http://www.crime research.org/news/28.03.2008/3277/.

71- Council of Europe, Convention on Cybercrime CETS NO.:185:http: // conventions .coe.int/ Treaty/Commun /ChercheSig.asp? NT=185&CM = &DF=&CL=ENG.

72- EWI Interview, March 2010.

73- Pedro Verdelho,“The Effectiveness of International Co-operation against Cybercrime: Examples of Good Practice, ” Discussion Paper (Draft), Project on Cybercrime, Council of Europe, March 12, 2008, http:// www.coe.int/t/dghl/ cooperation /economiccrime / cybercrime/ T-CY/DOC-567study4- Version7 _en.PDF.

74- Ibid.

75- For a list of examples of good practices, see ibid.

76- “Meeting of G8 Justice and Home Affairs Ministers, ” (Sea Island, GA.2004) http:// www.justice.gov/ criminal /cybercrime / g82004 /g8_back ground .html.

77- Ibid.

78- “Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, ” United Nationas General Assembly, 58th Session, A/Res/58/199, (January 30, 2004) http://www.itu.int/ITU D/ cyb/ cyber security / docs / UN_resolution_58_199 .pdf.

79- Virtuality Here: The Age of Cyber Warfare, McAfee, Inc. December 2009, http:// resources.mcafee.com /content/ NA Criminology Report 2009 NF

80- Ibid.

81- Jeffry Carr, Inside Cyber Warfare: Mapping the Cyber Underworld (Seattle:O’Reilly Media, 2009), p. 47.

82- McAfee, Virtuality Here.

83- Ibid.

84- Ibid.

85- “Treaty on Cyberwarfare—Is one needed?” Space and Telecom Law Faculty, University of Nebraska, PowerPoint presentation, available in PDF form at http:// spaceand telecomlaw.unl.edu/c/ document_library/get_file?folderId=1790400&name=DLFE-19052.pdf.

86- A. A. Streltsov, “International Information Security: Description and Legal Aspects, "International Disarmament Forum, no. 3,2007, http://www.unidir.org/pdf/articles/pdf-art2642.pdf.

87- “United States Views on Information Network and Infrastructure Security in the WSIS Action Plan.” World Summit on the Information Society, www.cyber security cooperation.org /.../WSIS-Security Position Paper-Handout_Version.doc.

88- Triin Parts, “2009—A New Beginning for The OSCE?, ” in Estonian Ministry of Foreign Affairs Yearbook 2008/2009, p. 42, http://web-static.vm.ee/static/failid/003/Triin_Parts.pdf.

89- Ibid., p. 42.

90- Ministerial Council Decision No. 2/09, Further OSCE Efforts to Address Transnational Threats and Challenges to Security and Instability, December2,2009: http:// www.osce.org / documents /cio/2009/12/41869_en.pdf.

91- Vice Chairman for the Joint Chiefs of Staff General James Cartwright, “Whither the Forward-Basing of U.S. Forces?” Quadrennial Defense Review,United States Department of Defense, Presentation at the Center for International and

Strategic Studies, June 4, 2009.http://www.defense.gov/ qdr/ transcripts_cartwright _20090604.html.

92- Daniel Korski, “Shaping a New NATO-Russia Partnership, ” SAIS enter for Transatlantic Relations:
http://transatlantic.sais-jhu.edu/bin/q/s/korski_Shaping_a_New_NATO-Russia_Partnership.pdf.

93- Quoted in Anders Aslund and Andrew Kuchins, “Pressing the ‘Reset Button’on US-Russia Relations, ” CSIS Policy Brief, March 2009.

94- See Project Grey Goose, “Russia—Georgia Cyber War: Findings and Analysis, ” Phase 1, 2008, p. 3.

95- Project Grey Goose, an NGO, was a forerunnerto the for-profit firm Grey Logic, both set up by Jeffrey Carr. , http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report.

96- Arie J. Schaap, “Cyber warfare operations: Development and use under international law, ” Air Force Law Review, December 22, 2009, http:// findarticles.com /p/articles/ mi_m 6007/is_64/ai_n42124173/?tag=content;col1.96 Martin C. Libicki, “Cyberdeterrence and Cyberwar, ” RAND, Project AirForce, 2009, http:// www.rand.org /pubs/monographs /2009/ RAND_MG77. sum.pdf.

97- Ibid.

98- Daniel Korski, “Shaping a New NATO-Russia Partnership.”

99- Ibid.

100- Carr, Inside Cyber Warfare, pp. 179–89.

101- Roy Mark, “House Passes Cybersecurity Act, ” Eweek.com,
March 2, 2010, http://www.eweek.com/c/a/Government-IT/House-Passes-Cybersecurity-Act-682741.

نبذة عن المؤلفين:

أولاً: فرانز ستيفن: هو احد أعضاء معهد دراسات الشرق والغرب. وقد عمل سابقاً في معهد الدراسات الإستراتيجية القومية في جامعة الدفاع الوطني في واشنطن الذي يركز في بحثه وتحليله على القضايا الأمنية الإقليمية. كما انه عمل محللاً في مشروع أصلاح الأمن القومي وهو منظمة غير ربحية ممولة من قبل الكونغرس بهدف أصلاح البنية الهيكلية للأمن القومي الأمريكي. حاز فرانز على شهادة الماجستير في الدراسات الإستراتيجية/ والاقتصاد الدولي من جامعة الدراسات الدولية المتقدمة وكذلك جامعة جونز هوبكنز، كما انه خدم في الجيش النمساوي ووزارة الخارجية النمساوية. وكرس جهده في القضايا الأمنية المتنوعة.

ثانيا: غريغ اوستين: وهو نائب رئيس برنامج التنمية والاستجابة السريعة في معهد دراسات الشرق والغرب. إن اهتماماته في الشؤون الدولية تمتد إلى ثلاثون عاماً وتتضمن تقلده المناصب العليا في المؤسسات الحكومية والأكاديمية. كما انه يقوم بكتابة عموداً/ مقالاً صحفياً في صحيفة أوربا الجديدة، بالإضافة إلى ما تقدم تقلد غريغ وظائف عليا في مجموعة الأزمات الدولية ومركزا السياسة الخارجية في لندن، كما انه ألف العديد من الكتب المهمة عن الأمن الدولي لاسيما حول أسيا. ومن اليكسي مارفيف، ويملك العديد من المؤهلات الأكاديمية العليا في العلاقات الدولية ومنها شهادة الدكتوراه، وتخصصه الرئيسي هو السياسة الأمنية للاتحاد السوفيتي وروسيا الاتحادية.

About the translator of this book :

- **Name**: Tareq Mohammed Dhannoon AL Taie

- **University Lecturer**: Specialist in(American–Russian Relations).

- **Working Place** :University of Mosul , College of Political Science , Dept. of International Relations.

- **Specialization** :

1- B.A :Political Science.(he ranked the second out of(57) students. got awarded the Degree of Bachelor in political Science grade (Excellent).

2- M.A :International Relations.(he ranked the first out of(5) students).

3- PhD in Progress : Strategy.(he ranked the first out of(7) students in (courses exams)

4- B.A: Degree of Bachelor in Translation into Arabic

- **Country** : Iraq

- **Book:**

1- The American – Russian Relations in the Post Cold War and their Future

- **Translated books:**

1- National Security Strategy of the Russian Federation to 2020. Approved By Decree of the President Of the Russian Federation 12 May 2009 No. 537.

2- The Foreign Policy Concept Of The Russian Federation: Approved by Dmitry A. Medvedev, President of the Russian Federation, on 12 July 2008.

3- Russia, The United States, And Cyber Diplomacy Opening the Doors: by Franz-Stefan Gady and Greg Austin.

- **Researches**

1-The effect of external factor in citizenship / publication / Journal of Regional Studies / Center for Regional Studies / University of Mosul.

2-The international dimensions of the U.S. missile shield project / publication / bulletin political Securities / Faculty of Political Science / University of Mosul.

3- International Crisis .

4- the Effects of European foreign policy toward the Israeli -Arab conflict .

5- The dialectical of relationship between the international system and international order /it has participated in the seminar hosted by the Faculty of Political Science / University of Mosul.

6- The Russian attitude towards of political change in the Arab world /it has participated in the seminar hosted by the Faculty of Political Science / University of Mosul.

7- others Researches

- **Conferences**: (8).

المحتويات